MEDIAWIJSHEID

Workshops voor kinderen en jongeren met een verstandelijke beperking over de thema's phishing, nepvrienden en cyberpesten.

MARYLINE VERSTRAETEN-NAUSCH,
EMMA PATTYN EN JONAS ZWAENEPOEL

1 Inhoudstafel

2 Inleiding

Deze bundel is opgemaakt door Jonas Zwaenepoel, Emma Pattyn en Maryline Verstraeten-Nausch, studenten aan de Arteveldehogeschool te Gent met de afstudeerrichting Bachelor Sociaal Werk. Wij kregen de opdracht om een workshop uit te werken met als thema 'veerkracht versterken bij personen met een beperking'. Voor ons leek dat het eerste moment een enorme uitdaging. Als groep hadden wij namelijk nog niet vaak contact met deze doelgroep.

Na een eerste ontmoeting met de organisatie Kompas, besloten wij ons toe te spitsen op mediawijsheid. Een thema dat vandaag de dag toch wel enorm belangrijk is met de toenemende digitalisering. Wij kozen er dan ook voor om het te hebben over thema's die de laatste periode enorm veel aandacht krijgen in de media. Deze zijn: phishing, cyberpesten en nepvrienden (identiteitsfraude).

Wij willen op een creatieve, speelse manier de deelnemers uitleg geven over deze thema's en vooral hen sensibiliseren zodat zij ook kunnen omgaan met de gevaren van de onlinewereld. Dit omdat wij de indruk hebben dat deze groep vaak wel eens vergeten wordt in deze thema's en zij daarom nog extra gevaar lopen om in valkuilen te trappen.

Wij zijn enorm enthousiast om deze workshops uit te schrijven. Helaas kregen wij als groep de melding dat wij vanwege corona de workshops niet fysiek mogen uitvoeren. Wij hebben toch geprobeerd om zo creatief mogelijk een oplossing te zoeken zodat de deelnemers en de organisatie in de toekomst de workshops kunnen uitvoeren. Wij hopen dat de organisatie gebruik kan maken van de werkvormen die wij neergeschreven hebben, alsook van de instructiefilmpjes zodat we op deze manier toch een verschil kunnen maken.

Bedankt aan Elisa Saman en Geertrui De Bruyne van vzw Kompas voor de feedback op onze workshops, dankzij jullie tips konden we onze workshops telkens verbeteren.

Ook een grote dankjewel aan onze begeleider van de Arteveldehogeschool Ann Ryckaert, voor de grote ondersteuning bij heel dit project.

3 Tips voor begeleiders

De uitwerking van de workshops werd gedaan op basis van een vooronderstelling dat deze fysiek konden gegeven worden aan de doelgroep, waarbij de begeleiders hulp konden bieden aan de deelnemers bij het deelnemen daar waar bijvoorbeeld teksten voorgelezen dienen te worden. Wij raden dan ook aan om indien mogelijk deze workshop zo veel mogelijk aan te bieden in het bijzijn van een begeleider of voogd ter ondersteuning van de instructievideo's.

De uitwerking van deze workshops is er gekomen door een toenemende vraag naar duiding over mediawijsheid om jongeren met een licht verstandelijke beperking wegwijs te maken in de digitale wereld. Dit is essentieel opdat zij op die manier niet uit de boot vallen. Wij trachten dan ook met dergelijke workshops ervoor te zorgen dat de doelgroep evenzeer kan deelnemen aan de digitale samenleving. Wij vinden het hierbij belangrijk om hen te wijzen op de valkuilen van media zoals onder andere de gevaren van **phishing, cyberpesten en nepvrienden.** Wij hebben getracht om niet te zeer over gevaren te spreken om de doelgroep niet af te schrikken en hen zoveel mogelijk te motiveren om de digitale wereld te ontdekken. Onze tip is dan ook om voorzichtig om te springen met de thema's. Er kan aan de deelnemers niet genoeg benadrukt worden dat de digitale wereld een mooie wereld is, zolang je je maar bewust bent van bepaalde zaken waar men best rekening mee houdt.

4 Workshop 1: Phishing

4.1 Doelstellingen

4.1.1 SMS & telefoon

- De deelnemers weten dat ze niet zomaar op een link in een sms mogen klikken.
- De deelnemers weten dat ze niet zomaar elke sms mogen vertrouwen.
- De deelnemers herkennen een telefoonnummer door te kijken naar de landcode.
- De deelnemers wetend at de Belgische landcode +32 is.

4.1.2 E-mail

- De deelnemers weten dat ze niet zomaar op linkjes mogen klikken.
- De deelnemers herkennen valse e-mails (kennen de belangrijkste weggevers van een valse mail).
- De deelnemers weten wat te doen wanneer je op een foute link klikt.

4.1.3 Andere vormen van phishing

- De deelnemers leren hoe ze een valse link kunnen controleren doormiddel van een gegeven website.
- De deelnemers leren de kenmerken van een valse link.
- Tijdens dit gedeelte leren de jongeren hoe ze een correct wachtwoord maken en wat de essentiële elementen zijn.

4.2 Materiaallijst

4.2.1 SMS & telefoon

- 20 Papiertjes met verschillende telefoonnummers en van verschillende landen.
- Verschillende afgeprinte sms'jes met smileys, linken, win-acties (een 10tal)
- Uitgedrukte kaartjes met pictogrammen/ korte woorden
    - Niet op een link klikken
    - Geen smileys
    - Belgische landcode

4.2.2 E-mail

- Voorbeelden echte mails (zie bijlage 2)
- Voorbeelden valse mails (zie bijlage 3)
- Rode map met vuilbak op
- Groene map met duim op

4.2.3 Andere vormen van phishing

- Voorbeelden correcte en frauduleuze websites.
- Kaartjes met vooraf vastgelegde woorden, cijfers en leestekens.

4.3 Algemene info over phishing

Phishing is een vorm van internetfraude die even oud is als het internet maar de laatste jaren ontzettend gegroeid is. Via phishing proberen criminelen gegevens los te krijgen van personen door onder andere websites na te bouwen van gekende bedrijven om op die manier geld lost te weken bij slachtoffers. Een andere gekende manier zijn het versturen van phishingmails en sms'en. Zo verzinnen cybercriminelen steeds nieuwe manieren om via e-mail of per telefoon achter je persoonlijke gegevens te komen en hiervan misbruik te maken. Ze proberen bijvoorbeeld je inloggegevens van je bank te bemachtigen om geld van je rekening te kunnen halen. Of ze proberen je te verleiden om persoonlijke gegevens terug te mailen of op een link te klikken.

Phishingmails en berichten zijn eng omdat ze steeds beter zijn en het kritisch er doorheen kijken vaak moeilijk is voor mensen met een (licht) verstandelijke beperking. Maar dat zou nooit iemand mogen tegenhouden om iets online te doen. Personen met een verstandelijke beperking zijn kwetsbaarder voor onder andere phishing dan personen zonder beperking, het is daarom belangrijk om hier extra aandacht aan te besteden zodat ook zij op een zo veilig mogelijke manier online kunnen deelnemen aan onze alsmaar meer gedigitaliseerde wereld.

4.4 Werkvorm voor de workshop

4.4.1 Inleiding

Hallo welkom, bedankt om aanwezig te zijn. *(de begeleiders stellen zich voor en de deelnemers stellen zich ook voor.)*

Wij komen vandaag een workshop geven over phishing. Vooraleer we beginnen hebben we enkele vragen voor jullie.

> Wie heeft toegang tot internet, gsm, computer?
> Hoeveel, wat, waarom?
> Weten jullie wat dat is, phishing?

Voor wie het nog niet kent, dat is helemaal niet erg.
Phishing is een vorm van internetfraude. Het woord is afkomstig van ‘vissen’, namelijk het vissen naar informatie of gegevens. Men probeert mensen op te lichten door ze te lokken naar valse websites, of via verschillende links. Ze proberen hier geld of persoonlijke gegevens te stelen.

Dit kan op verschillende manieren. Bijvoorbeeld via sms, e-mail, valse brieven, telefonisch en via nep-websites.

Straks gaan we in kleinere groepjes hier dieper op ingaan.

Hebben jullie het al eens meegemaakt dat mensen vragen naar persoonlijke gegevens? Heb jij al eens een vreemd sms'je ontvangen?

Phishing kan gebeuren bij iedereen. Het gebeurt enorm vaak en daarom komen wij vandaag uitleg geven en tips geven wat jullie kunnen doen als je een vreemd sms'je of e-mail krijgt.

Nu gaan we ons opdelen in groepjes met een doorschuifsysteem, iedereen zal informatie krijgen over de volgende onderdelen:
Dit groepje begint bij begeleider 1 heeft het over sms'jes en telefoontjes, het volgende groepje gaat bij begeleider 2 over wachtwoorden, het laatste groepje gaat bij begeleider 3 met en zal het hebben over mails..

4.4.2 Midden

4.4.2.1 Sms & telefoon (Begeleider 1)

Sturen jullie vaak berichtjes of whatsappjes?
Worden jullie dikwijls gebeld door nummers die jullie niet kennen?

Een andere naam voor phishing met berichtjes is 'smishing'. Je krijgt bijvoorbeeld een sms, een whatsapp- of facebookbericht met hierin een waarschuwing. (Bijvoorbeeld: "ben jij dit in deze video?") of ("Betaal nu of je rekening wordt geblokkeerd"). Dit kan ook een aanbieding zijn: "win een waardebon bij de Lidl".
Vaak moet je dan op een link (blauw en onderlijnd) klikken of terugbellen naar een telefoonnummer.
Ook kun je aan de telefoon te maken krijgen met een crimineel die zich voordoet als een officiële organisatie zoals je bank, of bijvoorbeeld mensen die iets willen kopen. Op deze manier proberen ze jouw persoonlijke gegevens te krijgen.

- Tips om phishing via de gsm of de telefoon te herkennen:
    - Let op het telefoonnummer. De twee cijfers na de + geven een landcode aan. Bij België is dit +32. Bij sommige gsm's komt er ook op van waar het telefoontje afkomstig is.
    - Let op schrijffouten.
    - Is het te mooi om waar te zijn?

- Vind je een telefoontje/bericht verdacht of raar? Stel jezelf dan deze vragen:
    - **Is het onverwacht?**

      Krijg je zonder reden een bericht van deze afzender: je kocht niets, had lang geen contact, enz. Controleer zeker verder.

    - **Is het dringend?**
    - **Ken je de afzender?**

Controleer het e-mailadres, ook op spellingsfouten. Maar let op: een officieel e-mailadres is nog steeds geen garantie.

- **Vind je de vraag vreemd?**

  Een officiële instantie zoals de overheid of bpost zal je nooit via e-mail, sms of telefoon vragen om je wachtwoord, bankgegevens of persoonlijke gegevens.

- **Naar waar leidt de link waar je moet op klikken?**

  Zweef met je muis over de link. Is de domeinnaam, het woord voor .be, .com, .eu, .org, … en voor de allereerste slash "/", ook echt de naam van de organisatie?

- **Word je persoonlijk aangesproken?**

  Berichten met algemene aanspreektitels (bijvoorbeeld: beste, dag …), of je e-mailadres als aanspreking, vertrouw je beter niet.

- **Bevat het bericht veel taalfouten?**

  Taalfouten of een vreemde taal kunnen wijzen op een verdacht bericht.

- **Probeert iemand je nieuwsgierig te maken?**

  Iedereen zou nieuwsgierig worden bij berichten met een link als "Kijk wat ik over jou las ..." of "Ben jij dit op deze foto?", maar laat je niet vangen.

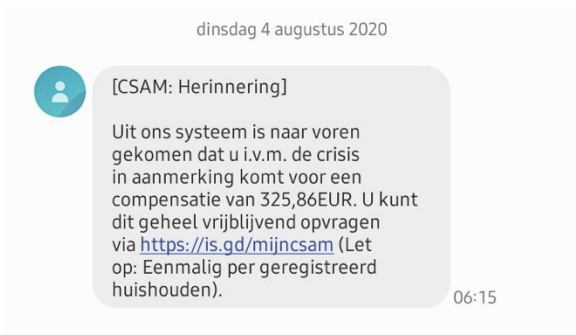
- **Vraag raad aan iemand anders wanneer je twijfelt!**

We doen de test!

Je krijgt een berichtje van Delhaize. Wat denken jullie van dit bericht? Wat vind jij raar?

Antwoord: Delhaize doet een winactie via WhatsApp. Er staat ook een hartje bij het bericht. Delhaize stuurt nooit zelf een bericht.

Je krijgt een berichtje van jouw bank. Wat denken jullie van dit bericht? Welke zaken vinden jullie raar?
Antwoord: Je krijgt een bericht van de bank. Dit is op zich al raar. Je kan een rare link zien. Bel best de bank zodat je zeker iemand van de bank aan de telefoon hebt of vraag hulp aan iemand.



Je krijgt een berichtje over de corona-tegemoetkoming. Wat denk je hiervan?

Antwoord: Er wordt via een berichtje geld aangeboden. Er staat een link in het berichtje.

Antwoord: Je krijgt nooit van officiële organisaties berichtjes via een normaal telefoonnummer. Wel via een telefoonnummer met maar 4 cijfers zoals '8000'. De bank of officiële organisaties zullen ook nooit via een bericht vragen om een blokkering op te heffen.

Antwoord: Stuur nooit geld naar iemand zonder dat je 100% zeker bent dat dit echt bijvoorbeeld jouw papa is. Beter ga je even langs bij de persoon die geld vraagt om dit echt zeker te zijn.

Werkvormen voor de begeleider:

Sms:

- Aandacht besteden aan: niet klikken op een link! Sms verwijderen!
- Een toneeltje: doen alsof je een raar sms'je krijgt en vragen wat je moet doen aan hen.
- Iemand van Kompas die hen sms'je stuurt en ze moeten aangeven waarom of waarom ze deze niet zouden openen.
- Uiteindelijk ook sms'jes voorleggen met bijvoorbeeld smileys in, een link, een soort win-iets en samen met hen op zoek gaan waarom dit wel of geen verdachte sms is. Werken met kaartjes/pictogrammen? (te mooi om waar te zijn, geen smileys bij officiële sms'en, niet drukken op linken)

Telefoon:

- Eerst samen bekijken hoe je een nummer herkent en wat de landcode van België is.
- Daarna enkele algemene voorbeelden bekijken met de algemene tips.
- Hierna een 20 tal telefoonnummers op tafel leggen en hen degene van België laten uithalen.
- Nooit je gegevens die niet iedereen mag weten doorgeven via de telefoon. Ook via een toneeltje doen alsof je naar iemand telefoneert van de groep.

4.4.2.2 E-mails (begeleider 2)

Inleiding

Dit deel gaat over phishing via e-mails. Dus: mensen die je persoonlijke gegevens willen te weten komen, en die dat doen aan de hand van valse e-mails versturen.

- Krijgen jullie veel e-mails? Ik krijg ook heel veel e-mails, en vooral veel reclame, **moeilijk om te weten wat een echte mail is**….

  Het is allereerst belangrijk om te weten dat je bank (bv. ING of BNP Paribas Fortis), je internetprovider (zoals bv. Telenet of Proximus) of andere organisatie nooit per e-mail vraagt om je inlogcodes of wachtwoorden door te geven. Krijg je de vraag, klik dus niet op een link in een e-mail die van een betrouwbare organisatie lijkt te zijn. Ze kunnen er bedrieglijk echt uitzien, zelfs met het logo van de organisatie.

Echte en valse e-mails onderscheiden

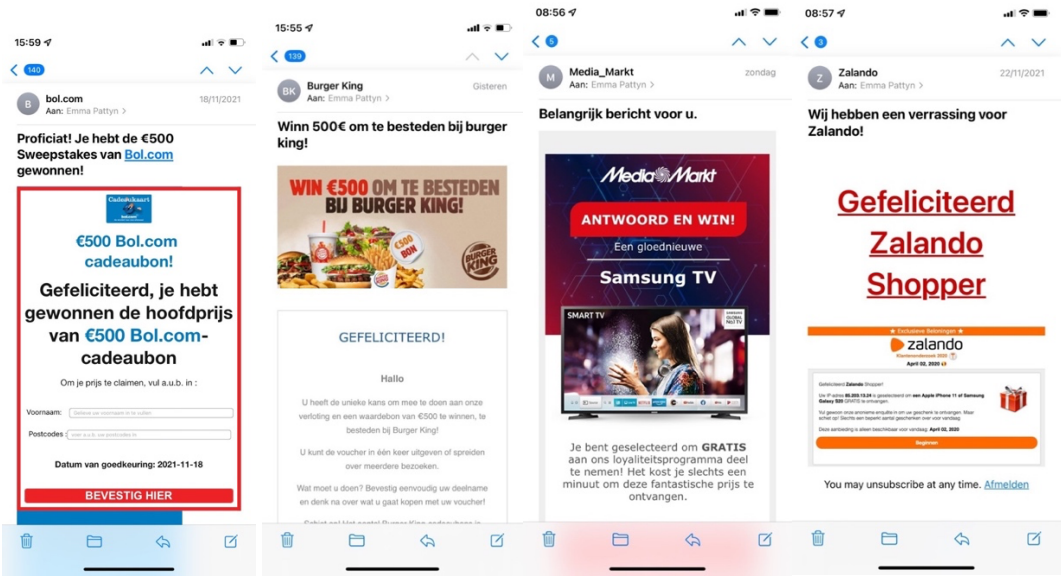
Vandaag de dag zijn er mensen die e-mails gebruiken om je te willen oplichten, dus hoe weet je eigenlijk of je een echte of valse mail krijgt?

De begeleider heeft voorbeelden van valse en echte e-mails bij (zie bijlage)

De begeleider heeft een **rode map met een vuilbak op en een groene map met een duim op** bij: de deelnemers steken de valse e-mails in de rode map en de echte mails in de groene map. De deelnemers leggen uit waarom ze denken of het een echte of valse e-mail is.

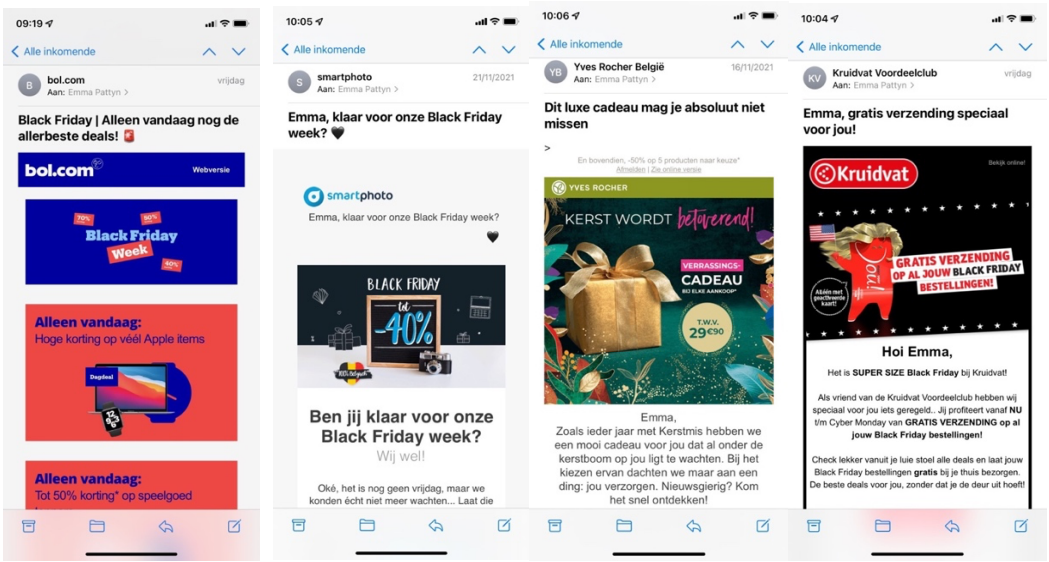
Voorbeelden van valse mails (zie bijlage)

- Bol.com
- Burger King
- Media Markt
- Zalando



Voorbeelden van echte mails (zie bijlage)

- Bol.com
- Smartphoto
- Yves Rocher
- Kruidvat



De begeleider overloopt de e-mails en toont waaraan je kan herkennen of het een valse e-mail is.

Hierbij een paar tips hoe je een nepmail kunt herkennen, de deelnemers bekijken de voorbeelden van mails om te kijken of ze die tips kunnen toepassen.

- **Algemene aanspreking**

  Word je aangesproken met hele algemene termen zoals 'Geachte heer/mevrouw' of 'Beste klant', let dan op. Als het wel echt het bedrijf of de instantie zou zijn waar je klant bent, dan staat in de aanhef meestal in ieder geval je achternaam en alleen 'heer' of 'mevrouw' ervoor, niet beide.

  Hoe zit dat bij de mails die jullie zien?

  - Bol.com vals: Geen aanhef
  - Media Markt: Belangrijk bericht voor u
  - Zalando: Zalando Shopper
  - Smartphoto, Yves Rocher, Kruidvat: Emma

- **Vraag om je persoonlijke gegevens**

  In veel nepmails staat het verzoek om op een linkje te klikken om je persoonsgegevens 'te controleren', 'bij te werken' of 'aan te vullen'. Ook kan je dan gevraagd worden in te loggen alsof je gaat internetbankieren. Doe dit nooit, want een crimineel kan je dan naar een valse website leiden en je persoonlijke gegevens in handen krijgen. Je bank, verzekeringsmaatschappij en overheidsinstanties vragen nooit via een e-mail naar persoonsgegevens. Je kunt het bedrijf of de instantie natuurlijk wel even bellen om te controleren of ze de e-mail hebben verstuurd. Gebruik hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

  - Bol.com vals: Naam invullen

- **Vraag om op linkjes te klikken of bijlage te openen**

  Criminelen die nepmails versturen, hopen dat je op de link in de mail klikt of dat je een bijlage opent. Want ze willen op deze manier schadelijke software op je computer installeren zonder dat jij het merkt. Een zip-bestand met bijvoorbeeld facturen of aanmaningen is altijd verdacht, want deze worden nooit op deze manier verstuurd. Verwacht je toch een bestand? Neem dan contact op met de afzender om te vragen wat en hoe ze iets precies verstuurd hebben. Gebruik ook hiervoor nooit de contactgegevens in de e-mail, maar zoek deze zelf op.

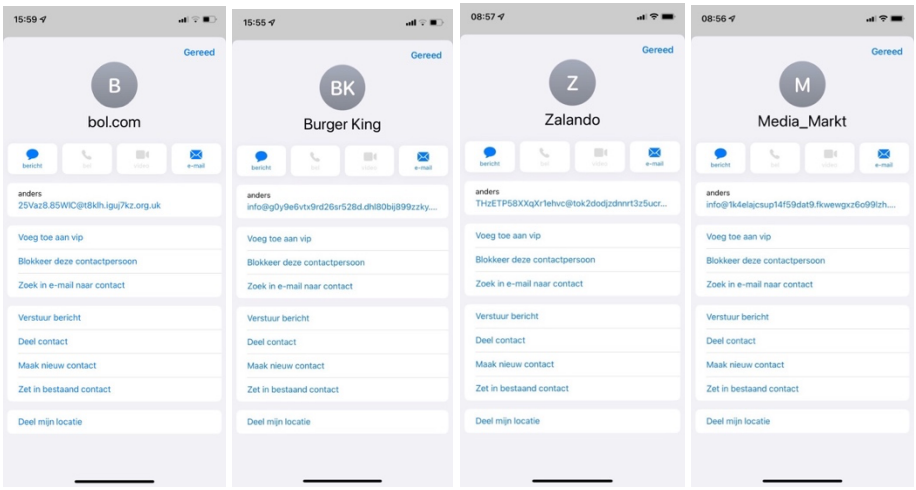
  - Bol.com vals: bevestig hier
  - Media Markt: Antwoord en win
  - Zalando: beginnen

- **Vaag of onduidelijk e-mailadres**

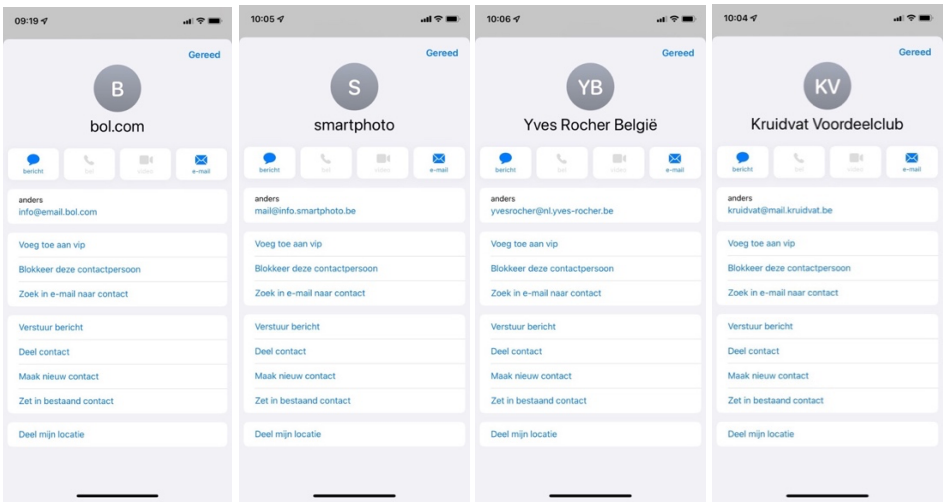
  Een nepmail heeft misschien een normaal ogende afzender zoals de naam van de webwinkel of je bank onderaan in de tekst staan, maar heeft vaak een onduidelijk e-mailadres als afzender. Bijvoorbeeld een afgeleide versie van de echte bedrijfsnaam. Controleer daarom het e-mailadres.

  De begeleider toont de e-mailadressen van de voorbeeldmails.

  Voorbeelden valse e-mailadressen (zie bijlage)



  Voorbeelden echte e-mailadressen (zie bijlage)



Na het overlopen van de tips steken de deelnemers de e-mails op de goede plek: in de rode of groene map.

Afsluiter: laatste tips

- Als we weten dat de afzender niet goed is, wat kunnen we dan doen? Blokkeren! Zo krijgen we geen mails meer in onze inbox van die persoon

- Wat als je toch op een link hebt gedrukt?
  - Je wordt naar een valse website geleid, daar mag je je **gegevens niet invullen**, of ze kunnen misbruikt worden om accounts over te nemen of geld te stelen
  - **Je zoekt beter zelf een website** in plaats van zomaar op linken te drukken

- Wat als je toch gegevens doorgaf?
  - Als je je wachtwoord hebt doorgegeven dat je op andere plaatsen gebruikt, verander het dan meteen.
  - Als je je bankkaartgegevens doorgaf, verwittig Cardstop (078170170) en contacteer je bank.
  - Als je merkt dat er geld is gestolen, doe aangifte bij de politie.

Werkvormen voor de begeleider:

- De begeleider begint met een openingsgesprek rond het ontvangen van veel e-mails.
- De begeleider deelt valse en echte e-mails uit, deelnemers steken ze in de bijhorende mappen.
- De deelnemers onderzoeken de e-mails na het horen van de tips om valse e-mails te ontmaskeren.
- De begeleider geeft tips mee

4.4.2.3 Wachtwoorden (begeleider 3)

Wachtwoorden

Een laatste belangrijk onderdeel waar ik het met jullie over zou willen hebben vandaag is over wachtwoorden. Op internet heb je namelijk vaak een wachtwoord nodig als je je wil aanmelden voor iets. Bij een **wachtwoord** is het belangrijk dat je dit zelf kan onthouden maar dat tegelijkertijd iemand anders jouw wachtwoord niet kan raden. Daarom dat ik vandaag enkele tips zou willen geven hierover. Waarom een goed wachtwoord belangrijk is wil ik jullie laten zien in het volgende filmpje:

https://www.youtube.com/watch?v=6uknozuNBG0&t=158s

Zijn er jullie enkele zaken opgevallen na het bekijken van het filmpje? Wat denken jullie dat je zeker nodig hebt om een goed wachtwoord te vinden dat je tegelijkertijd ook kan onthouden?

Ik heb enkele tips opgeschreven voor jullie die kunnen helpen voor een goed wachtwoord:

Gebruik nooit voor de hand liggende woorden zoals jouw naam, de naam van je mama, papa, broer of zus of getallen die op elkaar volgen zoals 123. Die zijn namelijk heel makkelijk te raden en dat is natuurlijk niet de bedoeling van ons wachtwoord.

Probeer een combinatie te maken van kleine letters, grote letters, cijfers en leestekens zoals een vraagteken of uitroepteken.

Maak een wachtwoord van minimaal 8 karakters. Dat is het minimum, hoe langer hoe beter.

Hiervoor kan je gebruikmaken van de kaartjes met woorden, leestekens en cijfers op.

Denk aan de tips die we gezien hebben:

- Gebruik **geen** opeenvolgende of aflopende cijfers in een wachtwoord, zoals **1,2,3 of 9,8,7**
- Probeer een combinatie te maken van kleine letters, grote letters, cijfers en leestekens zoals een vraagteken of uitroepteken.

Ik geef jullie enkele minuten de tijd om een wachtwoord uit te vinden door de kaartjes te combineren. Op die manier kan iedereen een wachtwoord uitvinden, zodat we zeker ons echt wachtwoord straks niet aan elkaar verklappen. Ik overloop straks samen met jullie mijn voorbeeld die we samen zullen bespreken.

4.4.2.4 Phishing via websites

Voorheen hebben wij gesproken over phishing per mail, sms en telefoon. Daarnaast werd het belang van een sterk wachtwoord meegegeven samen met de nodige tips.

Een andere manier van phishing die minder aan bod kwam is phishing via websites. Dit werd bewust weggelaten omwille van relevantie voor de doelgroep en complexiteit. We geven hier echter graag nog de link naar ***https://checkjelinkje.nl*** mee waar men een website link kan controleren op veiligheid. Deze site is ook toegevoegd op de kaart met tips voor de deelnemers.

De verdere verduidelijking van dit onderdeel werd ter info bijgevoegd als bijlage 7 bij het onderdeel phshing.

4.4.3 Slot

We herhalen de belangrijkste zaken nog eens.
Voorbeelden
Welke tips hebben jullie onthouden?
Wat hebben jullie bijgeleerd?
Zitten jullie nog met vragen?

Feedback vragen (hebben jullie iets bijgeleerd, vonden jullie het duidelijk,…)
Vonden jullie het leuk? Waarom?
Wat konden we beter of anders doen? Waarom?
Zouden jullie de volgende workshop over het thema phishing en mediawijsheid nog eens volgen? Waarom?
Willen jullie nog meer informatie over internetgebruik? Waarover?

Bedankt om zo goed mee te werken

5 Workshop 2: Cyberpesten

5.1 Doelstellingen

- Deelnemers weten wat cyberpesten is
- Deelnemers zien in waarom het fout is om te cyberpesten
- Deelnemers ervaren het effect van positieve commentaren en complimenten geven/krijgen
- Deelnemers weten wat te doen als ze te maken krijgen met cyberpesten

5.2 Materiaallijst

- Profiel voor elke deelnemer (zie bijlage)

5.3 Algemene info over cyberpesten

Cyberpesten is pesten via nieuwe media, zoals internet en gsm. Het kan bijvoorbeeld gebeuren via sms-berichten, sociale medianetwerken of via e-mail. We spreken van pesten als de dader de andere wil kwetsen, de dader meer macht heeft dan het slachtoffer en het negatieve gedrag vaak voorkomt.

Digitaal pesten kan op veel manieren. Online pesten mensen, vooral jongeren, elkaar door:

- Beledigen
- Misbruik van privégegevens (zoals het stelen van wachtwoorden of het aanmaken van nep-accounts)
- Uitsluiting in online groepen
- Het verspreiden van beeldmateriaal (zoals intieme foto's of filmpjes van mishandeling)
- Dreigtweets en haatposts

5.4 Werkvorm voor de workshop

Inleiding: kennismaking met begrip + eigen ervaringen

Vandaag hebben we het over cyberpesten. Weten jullie wat dat is? De begeleider legt uit wat cyberpesten is.

Heeft iemand van jullie/iemand die je kent al eens te maken gekregen met een cyberpester?

Heeft iemand van jullie al eens gemene dingen gezegd over iemand anders online?

In het echte leven ga je niemand pijn doen, ga je niemand uitschelden, dus online doen we dat ook niet!

Activiteit: over de streep

Alle deelnemers staan op 1 lijn en doen hun ogen dicht. De begeleider geeft hen situaties, en als ze die situatie kwetsend vinden, zetten ze een stap naar achteren, als ze die situatie grappig/leuk vinden zetten ze een stap naar voren.

De begeleider kan kiezen hoeveel situaties die gebruikt, afhankelijk van hoeveel tijd er voorzien is.

Situaties:

- Je post een gênante foto van iemand
- Jij wordt getagd in een lelijke foto
- Je krijgt een filmpje waarin iemand in elkaar wordt geslagen
- Een vriend van je liket al je foto's/posts
- Iemand fotoshopt een foto van jou op het lijf van een olifant
- Iemand stuurt je een roddel over iemand uit de groep
- Iemand zet jouw gsm-nummer online
- Iemand maakt in jouw plaats een Instagramaccount aan
- Je scheldt je vriend online uit voor 'dommerik'
- …

Daarna blijven de deelnemers op de plek staan waar ze zijn geëindigd en stelt de begeleider enkele vragen:

Zien jullie dat jullie op een andere plek staan?

Wat betekent dat?

> Iedereen vindt andere dingen grappig. Je weet niet wat iemand heel kwetsend kan vinden.

Houd je daar rekening mee als je online gaat?

De begeleider geeft de deelnemers enkele tips mee om cyberpesten te voorkomen.

Tips om (cyber)pesten te voorkomen

- Deel nooit privégegevens, zoals naam, adres, telefoonnummer of de naam van je school
- Scherm je profiel zoveel mogelijk af; 'alleen voor vrienden' is de beste optie
- Wees selectief in het accepteren van een vriendschapsverzoek; doe dit alleen wanneer je iemand in het echte leven ooit hebt ontmoet
- Verwijder onbekende mensen uit je vriendenlijst
- Houd wachtwoorden en inloggegevens altijd geheim: ook voor je beste vriend(inn)en
- Niet schelden en geen mensen kwetsen, dat zou je zelf ook niet leuk vinden
- Blokkeer degene die je lastig valt

Effect van positieve commentaren

Deelnemers hebben elk een ‘profiel’ zoals op Facebook (zie bijlage). Iedereen mag nu positieve dingen zeggen over elke deelnemer en de begeleider schrijft dat in kernwoorden in de tekstballonen op hun profiel.

Nadat iedereen complimenten kreeg, reflecteert de begeleider nog even over deze oefening:

Stel je voor dat we nu allemaal negatieve dingen hadden gezegd over elkaar, hoe zouden we ons dan voelen?

Nu kunnen we deze workshop eindigen met een goed gevoel!

6 Workshop 3: Nepvrienden

6.1 Doelstellingen

- De deelnemers weten dat er soms mensen op het internet zich voordoen als iemand anders.
- De deelnemers weten dat ze eerst moeten controleren of ze de persoon in het echt kennen.
- De deelnemers weten hoe ze een profiel moeten controleren.
- De deelnemers kennen de tips (of met behulp van de tipkaart) hoe ze nepvrienden kunnen herkennen.
- De deelnemers kennen de tips (of met behulp van de tipkaart) hoe ze zichzelf moeten beschermen op het internet tegen nepvrienden.

6.2 Materiaallijst

- Tipkaart om nepvrienden te herkennen.
- Valse en echte profielen

6.3 Algemene info over nepvrienden (identiteitsfraude)

Wat zijn nepvrienden:

Nepvrienden zijn mensen die zich op het internet voordoen als iemand anders. Dit gebeurt voor verschillende redenen. Sommige mensen willen graag iemand anders zijn, anderen willen mensen in de val lokken voor geld of een relatie. Ze doen zich vaak voor als vrienden. Vertrouw niks toe wat je ook niet zou toevertrouwen aan vreemden op straat.

Tips om nepvrienden te herkennen:

Controleer als eerste of je de persoon in het echt ook kent. Ken je deze persoon niet, dan is het beter dat je geen persoonlijke gegevens deelt.

Controleer als tweede de profielfoto. Lijkt dit een foto van iemand anders? Heeft de persoon maar 2 foto's van hem/haar op bijvoorbeeld Facebook? Dan vertrouw je dit beter niet.

Tips om jezelf te beschermen:

Stuur nooit persoonlijke gegevens door naar iemand die je niet kent. Zelf iemand die je kent hoeven deze niet te weten, deel dit enkel met personen die je echt kan vertrouwen zoals je ouders of vaste begeleiders.

Geef ook nooit geld uit online. Indien je iets online wil bestellen, doe dit dan met iemand die je kent zodat je zeker bent dat je geen geld verliest.

Deze tips zullen we aanbrengen door een tipkaart.

6.4 Werkvorm voor de workshop

De begeleiders maken verschillende accounts aan of maken gebruik van de accounts bijgevoegd in de bijlagen. Ze leggen enkele nepaccounts voor waar ze samen op zoek gaan met de deelnemer als een soort ‘cluedo’ wie nep is en wie niet.

Nepaccounts die je kan maken: Account met profielfoto van Koen Wouters, account met helemaal niets op, ...

Er zitten screenshots van valse en echte accounts in de bundel zodat de organisatie deze kan gebruiken.

Eerst zal je de deelnemers wat info geven over wat nepvrienden zijn en hoe je deze herkent. Je geeft hen ook tips over hoe ze moeten ontdekken of iemand een vals account heeft of niet. Dan ga je samen aan de slag met de ‘cluedo’ waar je stap voor stap bekijkt of het al dan niet een vals account zou kunnen zijn. Je leert de deelnemers ook dat als ze het niet 100% zeker zijn, ze beter geloven dat het een nepaccount is.

Kijk nu zelf even naar jouw vrienden op Facebook. Merk je hier enkele ‘nepvrienden’ op?

Op het einde overloop je nog eens alle tips en vraag je aan de deelnemers wat ze vooral onthouden hebben.

7 Interessante bronnen voor begeleiders

Netwerk Mediawijsheid. (2020). *Online met een licht verstandelijke beperking? De startgids voor een leuk en veilig online leven.* Opgeroepen op Oktober 2021, van Netwerk Mediawijsheid: https://netwerkmediawijsheid.nl/wp-content/uploads/sites/6/2020/10/Online-met-een-licht-verstandelijke-beperking-startgids-voor-een-leuk-en-veilig-online-leven_Netwerk-Mediawijsheid.pdf

Mensen met een licht verstandelijke beperking zijn online kwetsbaar: ze zijn vaker slachtoffer én dader van online misstanden zoals **cyberpesten, sexting en grooming**. De bron zegt dat leven zonder internet geen optie is in onze digitale wereld. Mediawijsheid en digitaal burgerschap zijn van cruciaal belang als je daar optimaal gebruik van wilt maken. Sociale media helpen mensen met een LVB om **gevoelens van eenzaamheid te verminderen, beter te integreren in de samenleving én om nieuwe vaardigheden aan te leren en hun zelfvertrouwen te vergroten.**

Mensen met een beperking geraken door de complexe digitalisering achterop, en daarom is het belangrijk hen juist mee te nemen in zowel **kansen als risico's van sociale media**.

7.1 Phishing

https://www.vpngids.nl/veilig-internet/cybercrime/wat-is-phishing/

Dit artikel geeft op een duidelijke manier weer wat de essentie van phishing is. Het artikel geeft verschillende voorbeelden en somt de belangrijkste aandachtspunten op.

7.2 Cyberpesten

https://www.klasse.be/217173/cyberpesten-6-vormen/

In dit artikel van Klasse worden verschillende vormen van cyberpesten toegelicht. Cyberpesten heeft over het algemeen meer impact dan offline pesten. Het is voor omstaanders vaak moeilijker op te merken, omdat de schade online gebeurt. Er zijn verschillende vormen van cyberpesten.

https://www.mediawijs.be/nl/dossiers/cyberpesten

Mediawijs heeft een pagina over cyberpesten, met veelgestelde vragen beantwoord. De pagina heeft ook onderzoekscijfers en biedt handige tools aan, zoals een stappenplan bij cyberpesten. Deze website is een handige samenvatting, met alle info die je nodig hebt wanneer je het thema 'cyberpesten' ontdekt.

7.3 Nepvrienden

https://www.mediawijsheid.nl/veilig-internet/

Hierboven vindt u een artikel die dieper ingaat op 'hoe veilig omgaan op het internet'. Er wordt ook wat info gegeven over contact met onbekenden die heel nauw aansluit bij de workshop rond nepvrienden. Dit is wel van een Nederlandse website, dus niet alle organisaties bestaan ook in België. Wel kan je altijd terecht bij de politie.

Contact met (on)bekenden

Op internet is het mogelijk om contact te leggen met mensen over de hele wereld. Met bekenden maar ook met onbekenden. Hoe weet je of iemand op internet echt is wie die zegt te zijn? En of je iemand kunt vertrouwen? ***Bedenk bij online contact met onbekenden: vertrouw niets toe, wat je aan een vreemde op straat ook niet zou toevertrouwen****. En vraagt een bekende via een appje om een groot bedrag te betalen? Wees dan alert op identiteitsfraude.*

Tips om identiteitsfraude te voorkomen:

Bij identiteitsfraude doet een oplichter zich voor als iemand anders. Hiervoor worden de naam, profielfoto en andere persoonlijke gegevens misbruikt. Bijvoorbeeld om een duur abonnement af te sluiten of om een rekening te openen.

Een veelgebruikte manier om aan gegevens te komen is phishing. Maar ook gegevens die je zelf op internet zet, bijvoorbeeld op je sociale media profiel, kunnen worden misbruikt. Let daarom goed op welke informatie je online deelt en wie dit kan zien.

- *Zet zo min mogelijk persoonlijke gegevens online*
- *Koppel accounts niet aan elkaar*
- *Verstuur je een kopie van je identiteitsbewijs? Rijksoverheid biedt tips om dat veilig te doen*
- *Vergroot je privacy met deze tips*

Ook kan het zijn dat een bekende in je omgeving te maken heeft met identiteitsfraude. Wees daarom alert als een bekende je via een appje of mail vraagt om een groot bedrag over te maken. Veiliginternetten.nl geeft tips om hulpvraagfraude via WhatsApp te herkennen en voorkomen
Wat te doen als het misgaat?

- *Doe aangifte bij het meldpunt identiteitsfraude*
- *Tips van Google om identiteitsdiefstal te voorkomen*
- *Meldpunt.nl legt uit wat je kunt doen bij identiteitsfraude*

7.4 Referentielijst

Douma, J. (2018, Februari). *Jeugdigen en (jong)volwassenen met een licht verstandelijke beperking.* Opgeroepen op Oktober 2021, van Landelijk Kenniscentrum LVB: https://www.kenniscentrumlvb.nl/wp-content/uploads/2019/02/Jeugdigen-en-jongvolwassenen-met-een-LVB.pdf

Fastenau, K. (2020, Februari 12). *Cyberpesten: ken jij deze 6 vormen van online pesten al?* Opgeroepen op Januari 2022, van Klasse: https://www.klasse.be/217173/cyberpesten-6-vormen/

Netwerk Mediawijsheid. (2020). *Beroepskrachten over het mediagebruik van jeugdigen met een beperking.* Onderzoek. Opgeroepen op Oktober 2021, van Netwerk Mediawijsheid: https://www.nji.nl/system/files/2021-04/Beroepskrachten-over-mediagebruik-jeugdigen-met-een-beperking.pdf (24 pagina's)

Reintjens, M. (2020, Juni 12). 'De "knoppenkennis" is er wel, maar het ontbreekt aan mediawijsheid'. Christen Democratische Verkenningen. (volledig artikel)

Vandevelde, L. (2016). BUITENGEWOON ONLINE. KWALITATIEF ONDERZOEK NAAR HET GEBRUIK VAN FACEBOOK DOOR PERSONEN MET EEN LICHT TOT MATIG VERSTANDELIJKE BEPERKING. Gent: Universiteit Gent. (Pagina 21-32 en pagina 41-67)

mediawijsheid.nl. (sd). Online met een beperking. Opgehaald van mediawijsheid.nl: https://www.mediawijsheid.nl/beperking/ (opgehaald 22/10/2021 - volledig artikel)

Netwerk Mediawijsheid. (2020). *Online met een licht verstandelijke beperking? De startgids voor een leuk en veilig online leven.* Opgeroepen op Oktober 2021, van Netwerk Mediawijsheid: https://netwerkmediawijsheid.nl/wp-content/uploads/sites/6/2020/10/Online-met-een-licht-verstandelijke-beperking-startgids-voor-een-leuk-en-veilig-online-leven_Netwerk-Mediawijsheid.pdf (28 pagina's)

David, J. (2021). *Samenvatting: wat is phishing*. Opgehaald van VPN Gids. https://www.vpngids.nl/veilig-internet/cybercrime/wat-is-phishing/

8 Slot

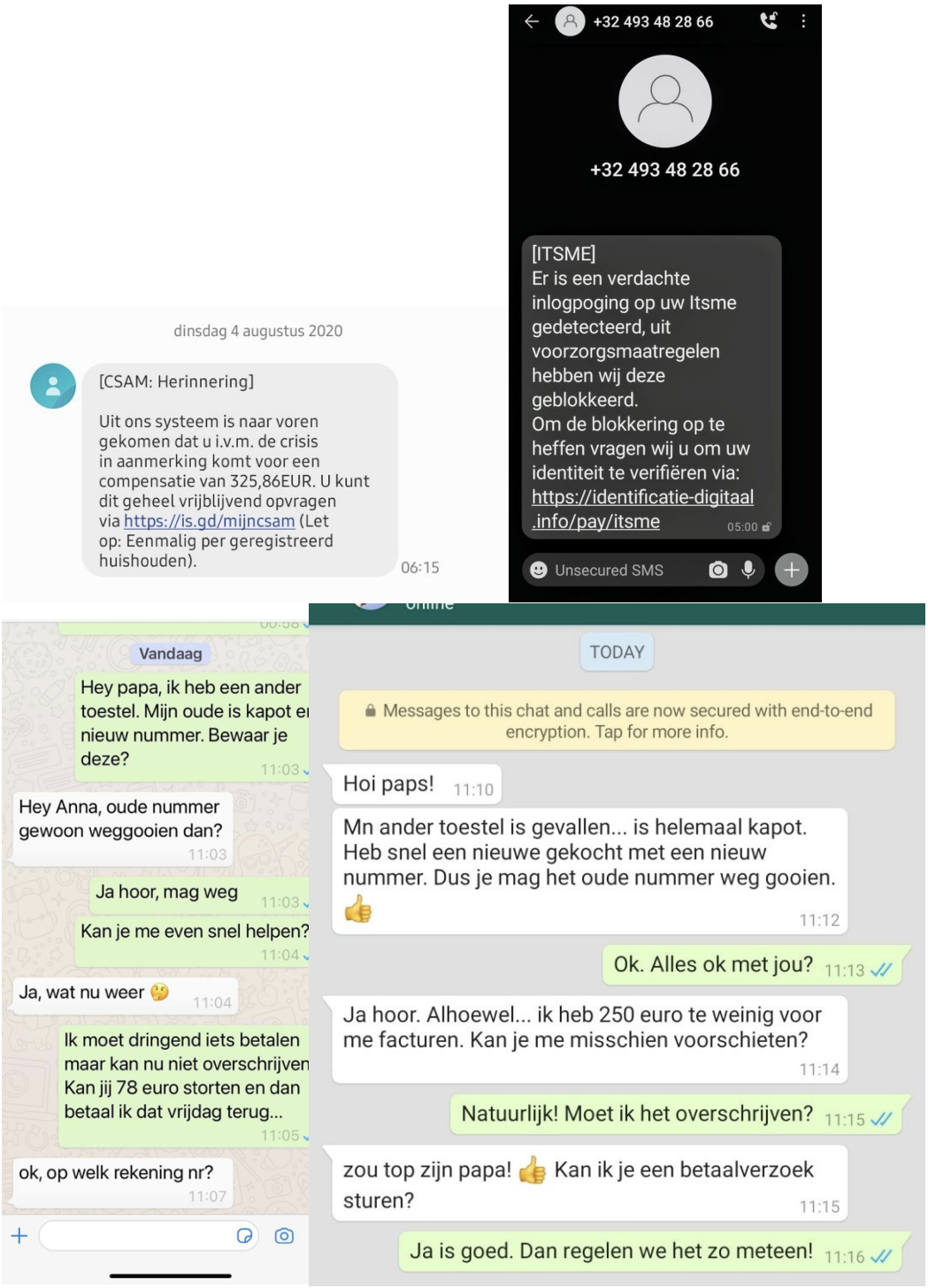
Het is belangrijk het thema mediawijsheid aan te kaarten, zeker bij deze doelgroep. We hopen dan ook dat de workshops een goede manier zijn om mensen met een verstandelijke beperking iets bij te leren hierover.

We vonden het heel jammer dat we onze workshop uiteindelijk niet zelf konden geven. We werkten al die tijd toe naar een spannend moment, dat uiteindelijk niet kon doorgaan. Gelukkig was ons werk niet voor niets, en mag het voortleven in de vorm van onze instructievideo's en deze bundel.

9 Bijlagen

9.1 Phishing

9.1.1 Bijlage: Sms'en



9.1.2 Bijlage: telefoonnummers

+32468940644

+32422557756

+31473585263

+20567893056

+27345789675

+32468938672

+52434763411

+32478935621

+31597492679

+32456667824

+52467225583

+32451214095

+91467912461

+90491084932

9.1.3 Bijlage: Valse e-mails

1. Bol.com

2. Burger King

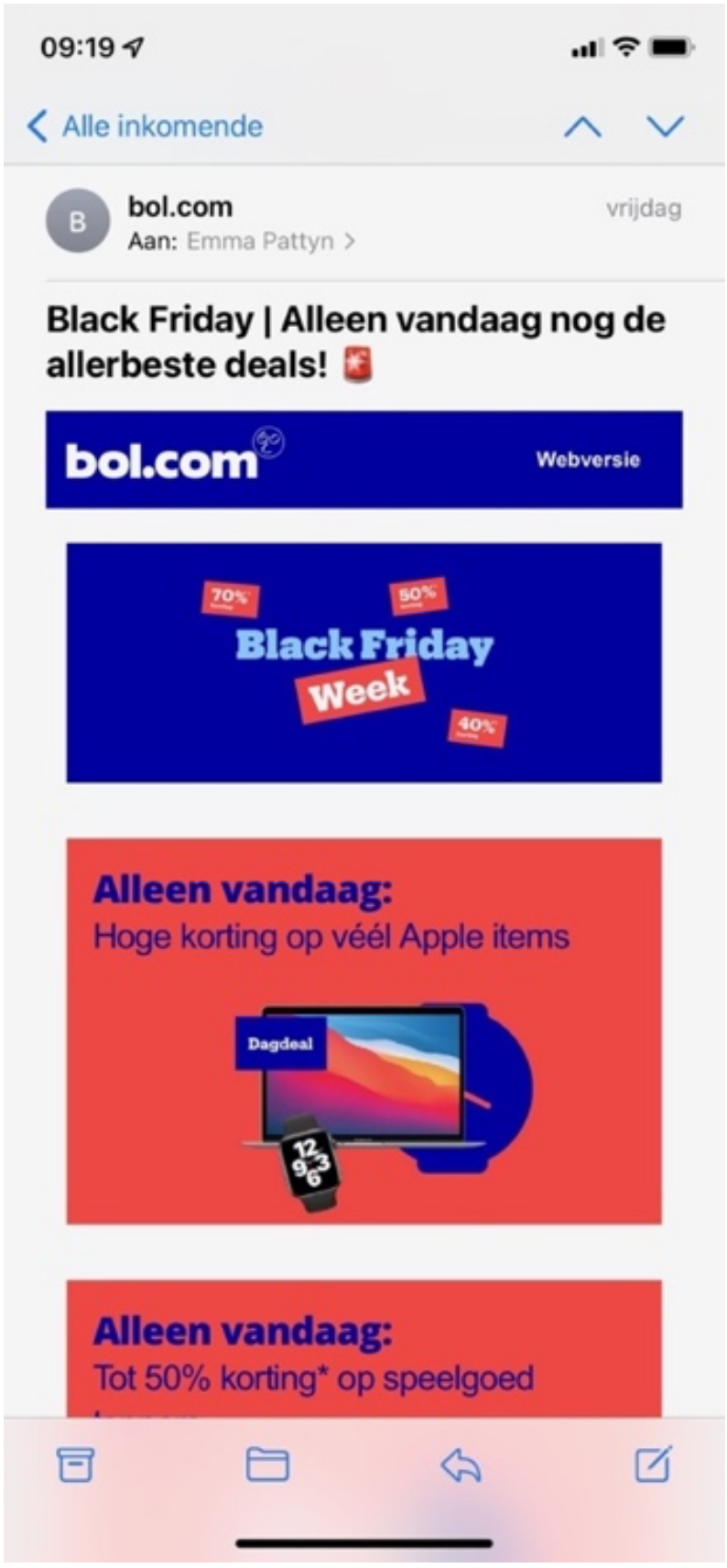
3. Mediamarkt

4. Zalando

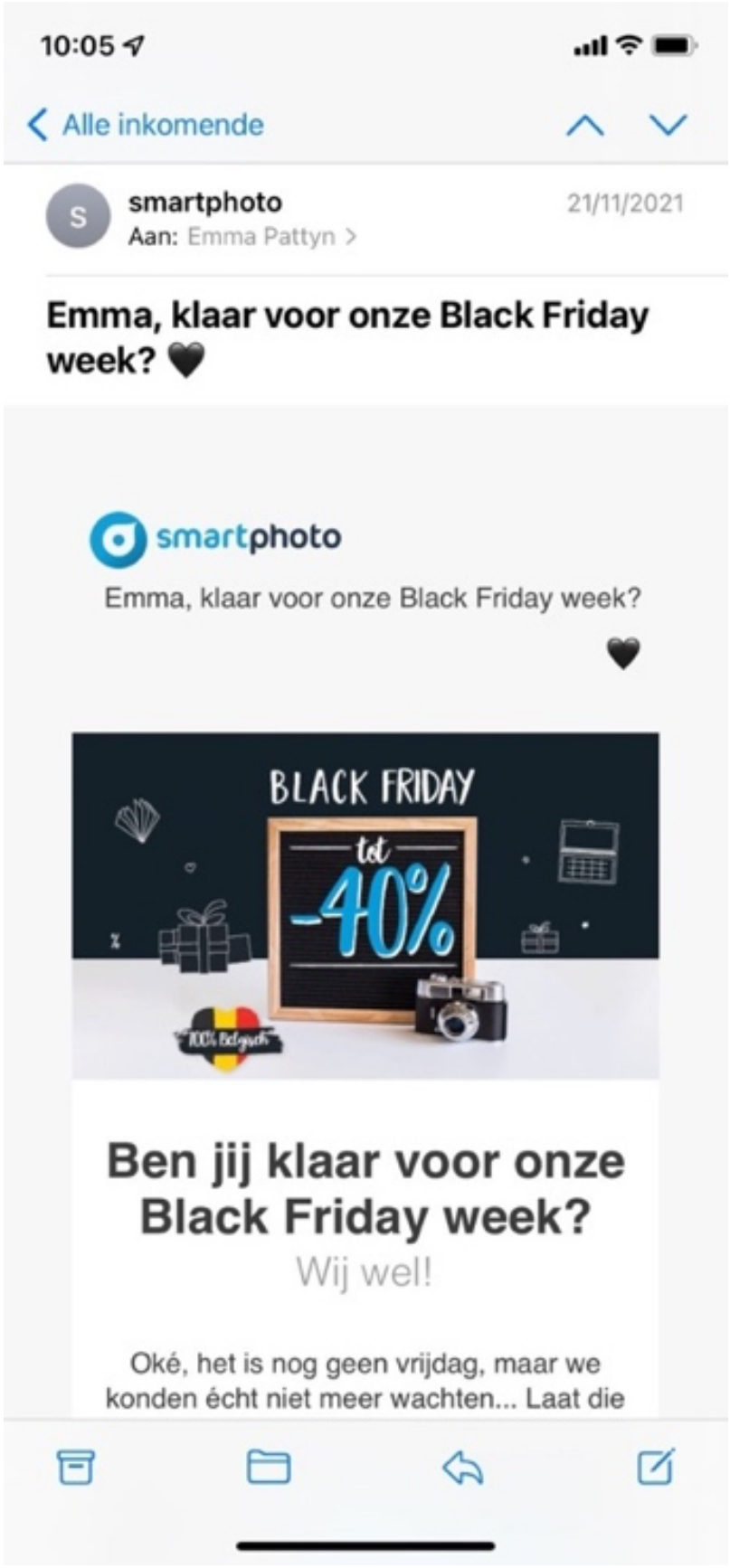

08:57
3
Z
Zalando
Aan: Emma Pattyn >
22/11/2021
Wij hebben een verrassing voor Zalando!
Gefeliciteerd
Zalando
Shopper
★ Exclusieve Beloningen ★
zalando
Klantenonderzoek 2020
April 02, 2020
Gefeliciteerd Zalando Shopper!
Uw IP-adres 85.203.13.24 is geselecteerd om een Apple iPhone 11 of Samsung Galaxy S20 GRATIS te ontvangen.
Vul gewoon onze anonieme enquête in om uw geschenk te ontvangen. Maar schiet op! Slechts een beperkt aantal geschenken over voor vandaag.
Deze aanbieding is alleen beschikbaar voor vandaag: April 02, 2020
Beginnen
You may unsubscribe at any time. Afmelden

9.1.2 Bijlage: Echte e-mails

1. Bol.com



2. Smartphoto



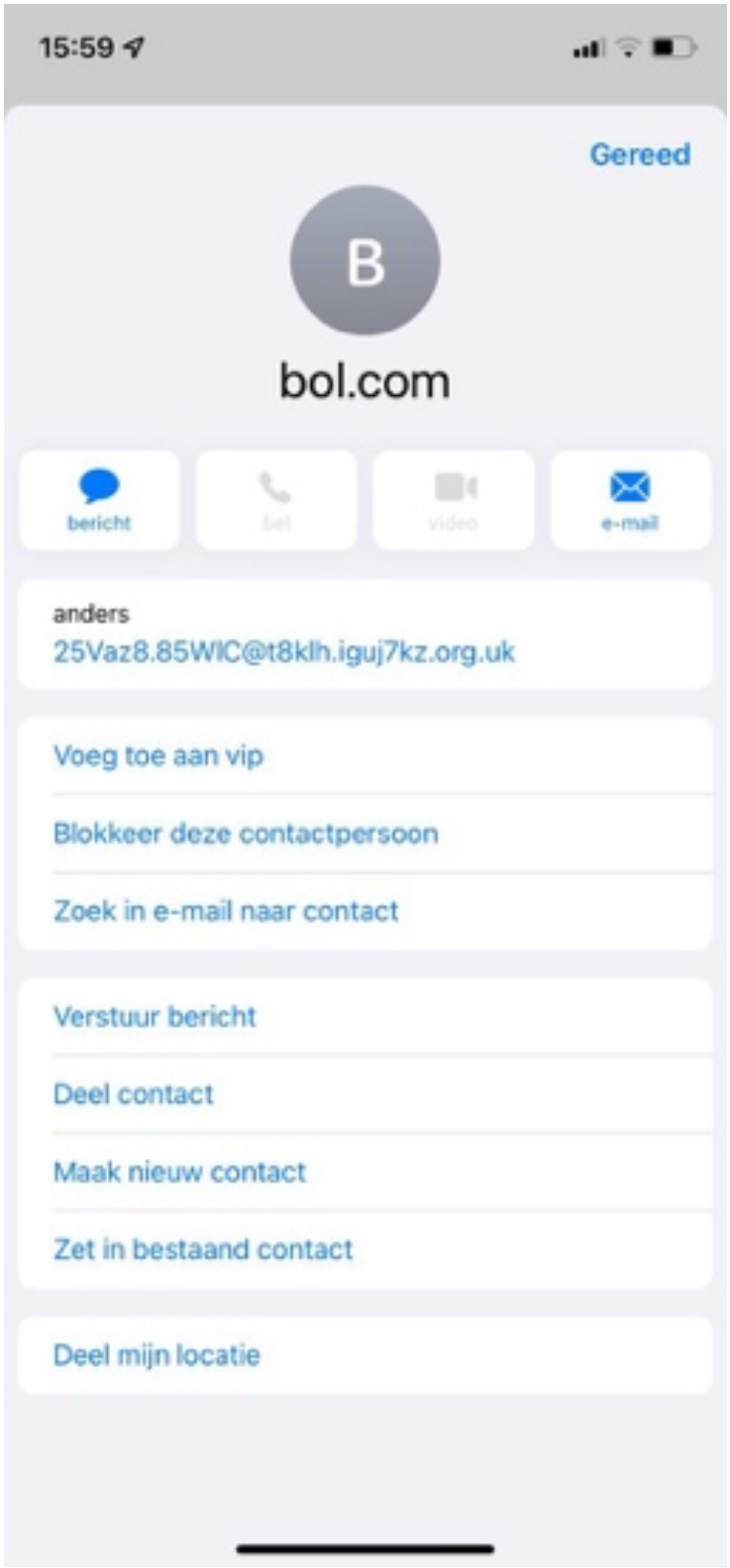
3. Yves Rocher

4. Kruidvat

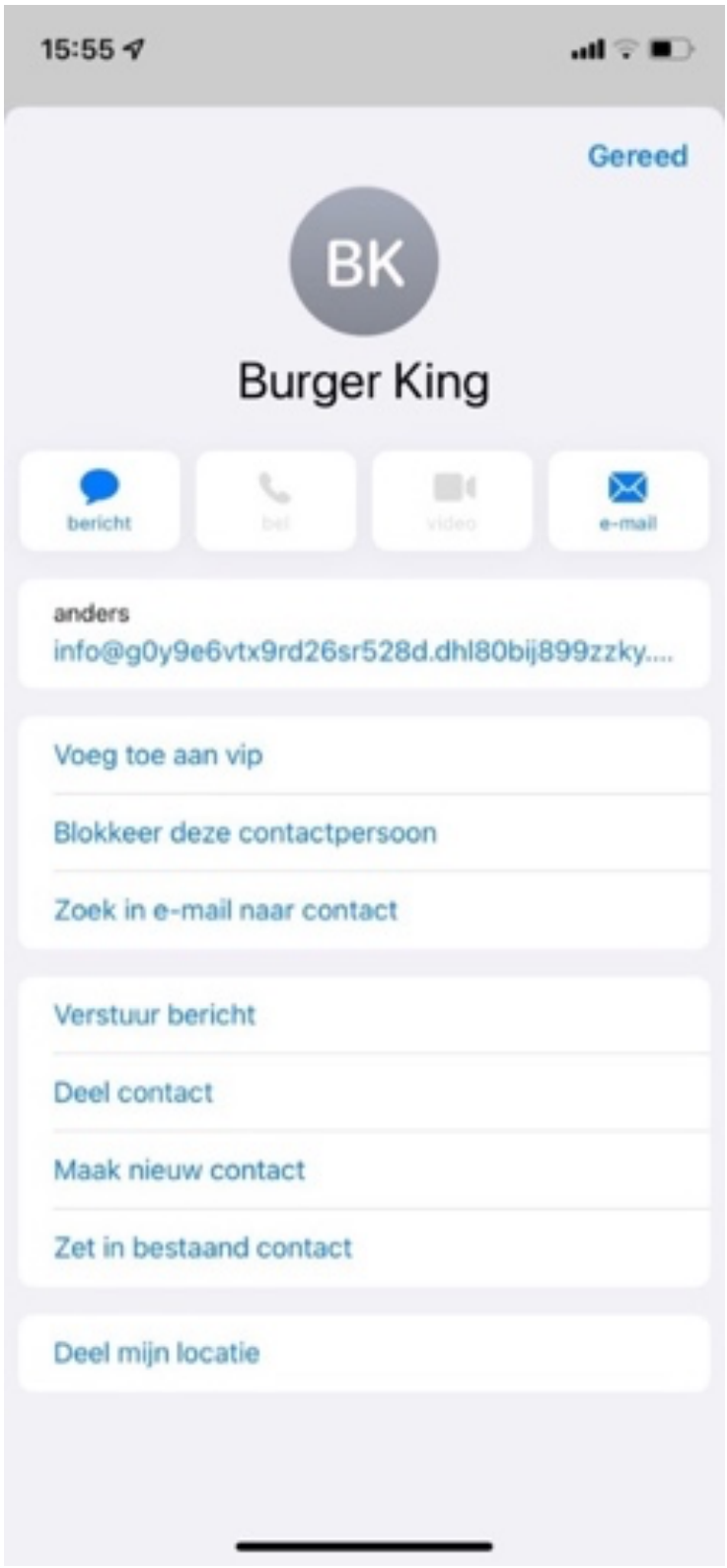

10:04
Alle inkomende
KV
Kruidvat Voordeelclub
vrijdag
Aan: Emma Pattyn
Emma, gratis verzending speciaal voor jou!
Kruidvat
Bekijk online!
GRATIS VERZENDING OP AL JOUW BLACK FRIDAY BESTELLINGEN!
Alléén met geactiveerde kaart!
Hoi Emma,
Het is SUPER SIZE Black Friday bij Kruidvat!
Als vriend van de Kruidvat Voordeelclub hebben wij speciaal voor jou iets geregeld.. Jij profiteert vanaf NU t/m Cyber Monday van GRATIS VERZENDING op al jouw Black Friday bestellingen!
Check lekker vanuit je luie stoel alle deals en laat jouw Black Friday bestellingen gratis bij je thuis bezorgen. De beste deals voor jou, zonder dat je de deur uit hoeft!

9.1.3 Bijlage 3: Voorbeelden valse e-mailadressen

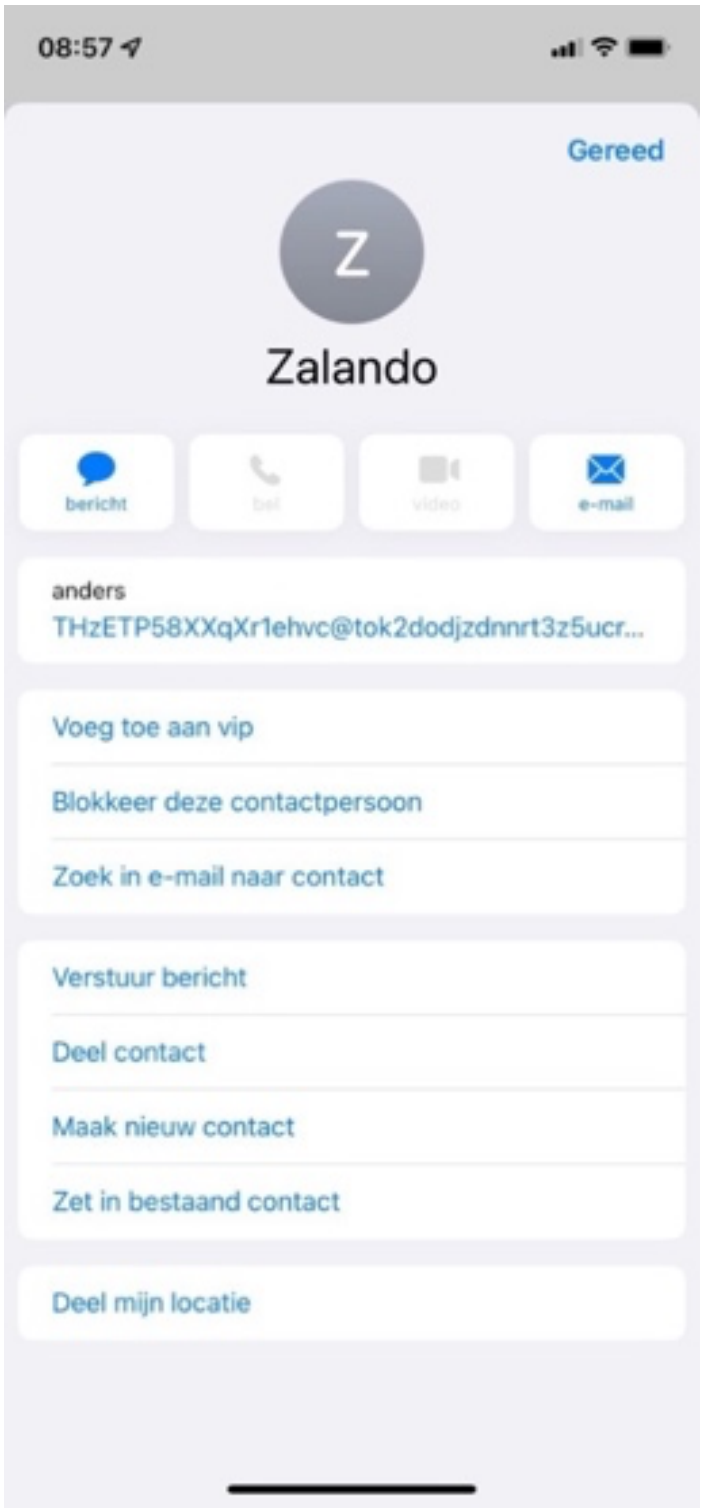
1. Bol.com



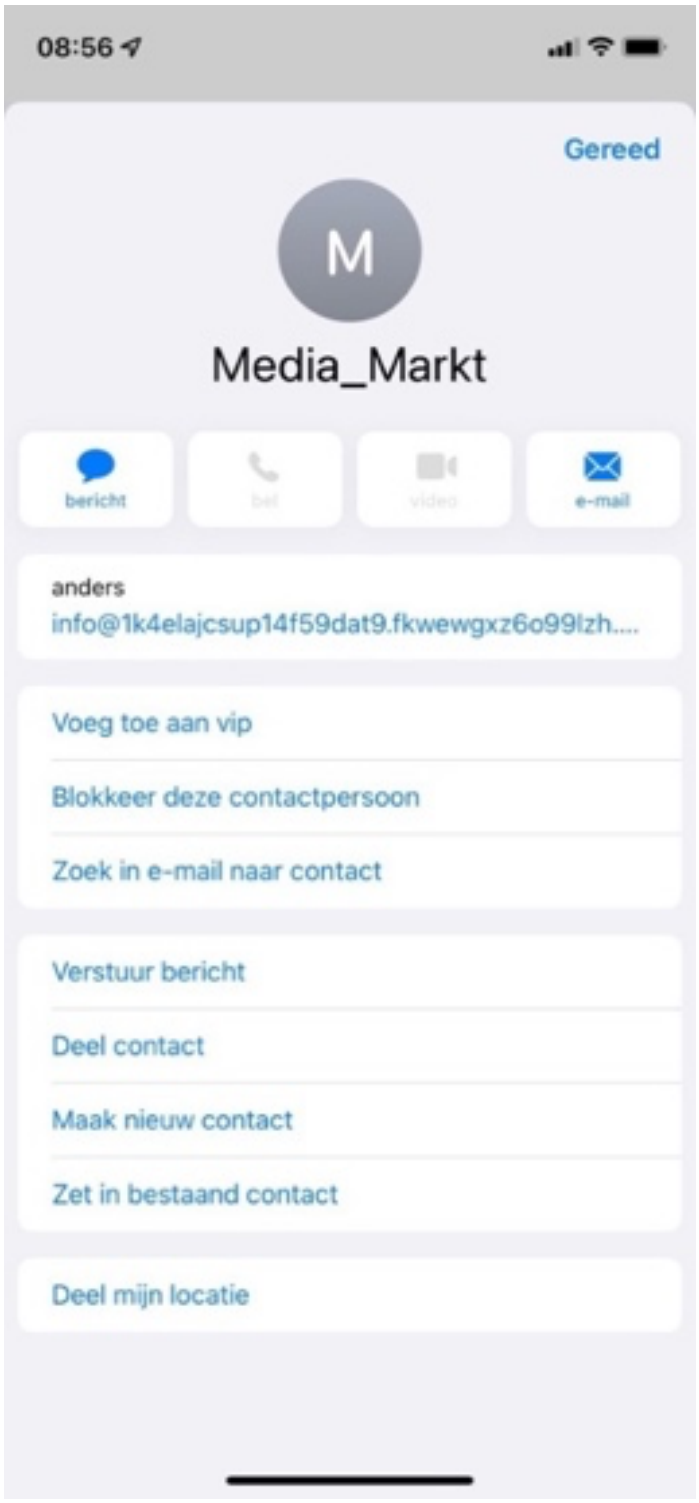
2. Burger King


15:55
Gereed
BK
Burger King
bericht
bel
video
e-mail
anders
info@g0y9e6vtx9rd26sr528d.dhl80bij899zzky....
Voeg toe aan vip
Blokkeer deze contactpersoon
Zoek in e-mail naar contact
Verstuur bericht
Deel contact
Maak nieuw contact
Zet in bestaand contact
Deel mijn locatie

3. Zalando

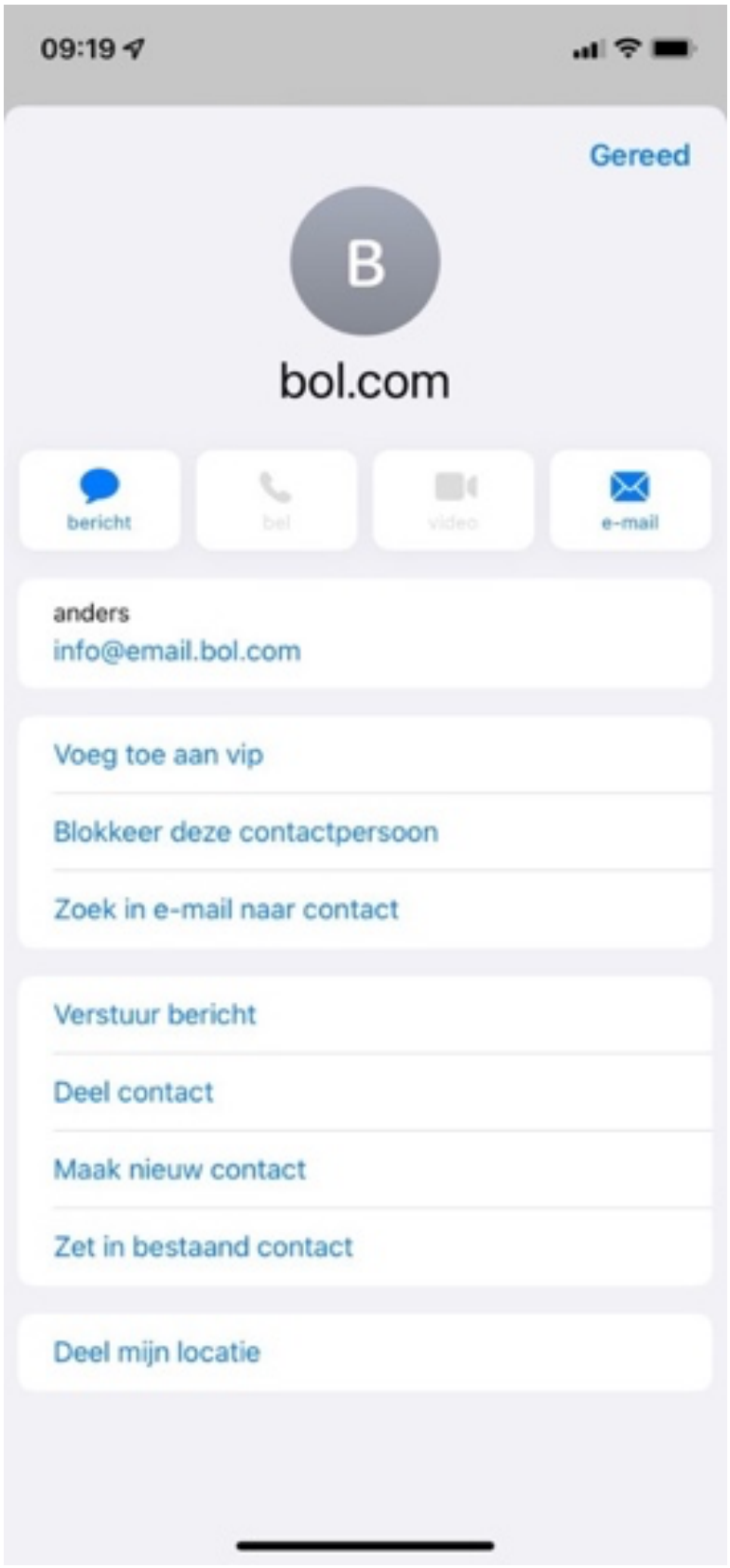


4. Media Markt

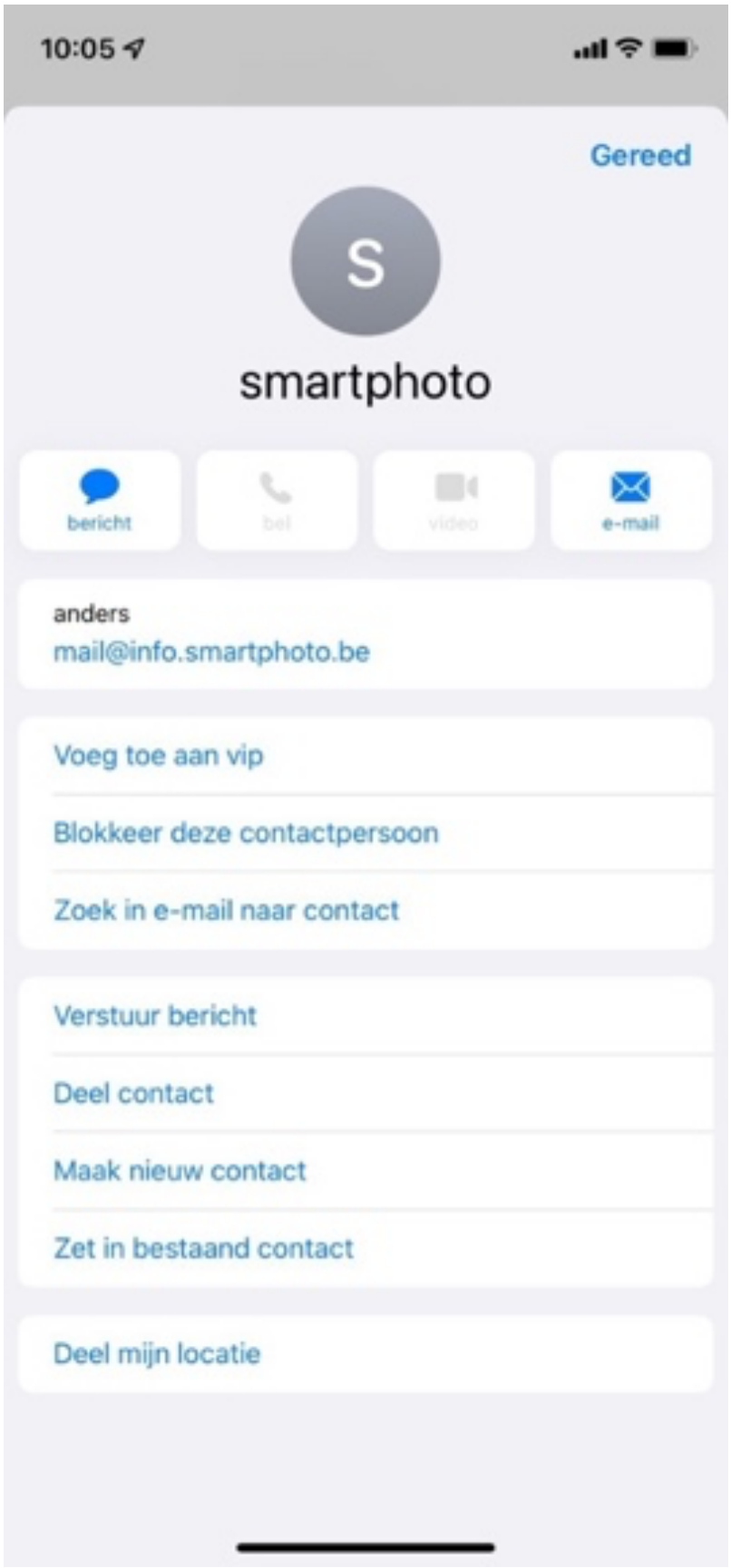


9.1.4 Bijlage 4: Voorbeelden echte e-mailadressen

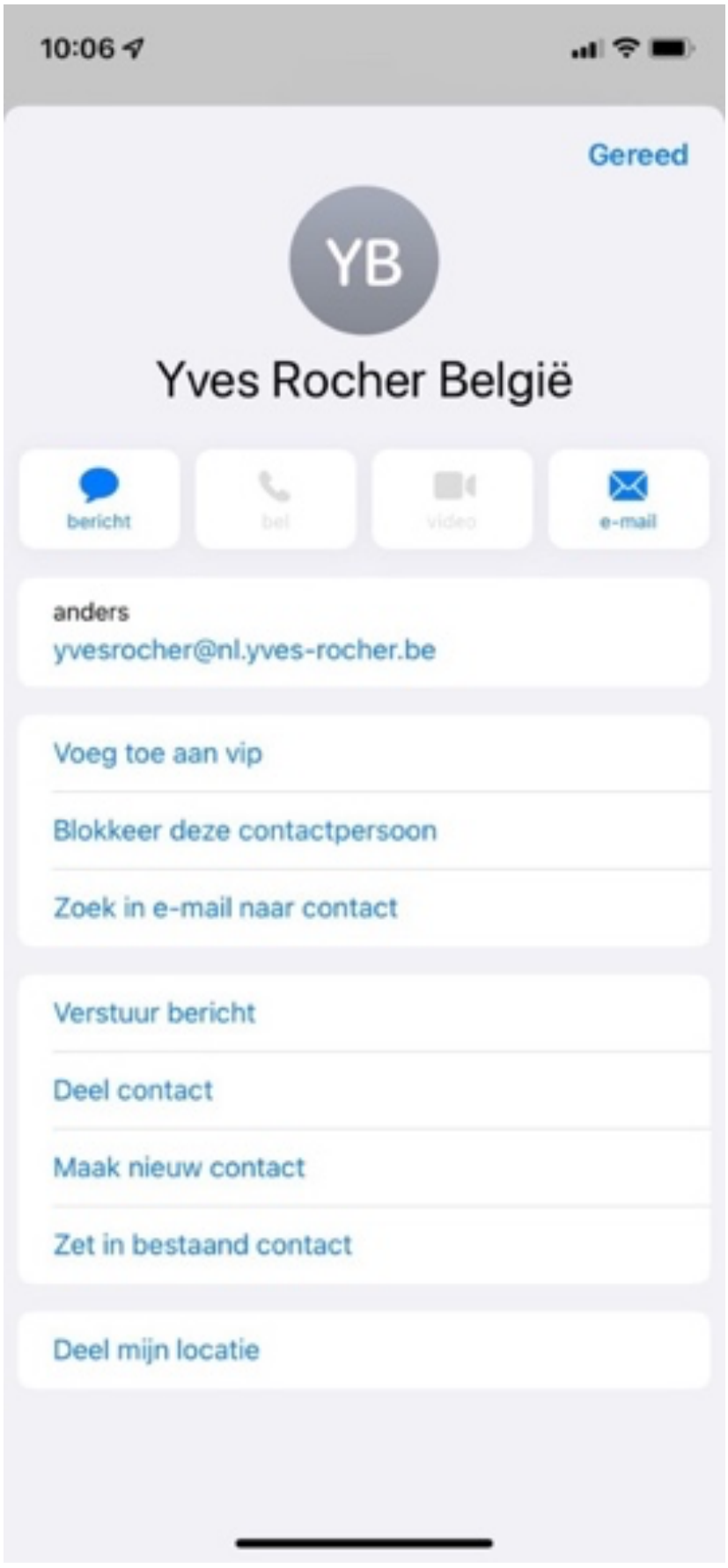
1. Bol.com



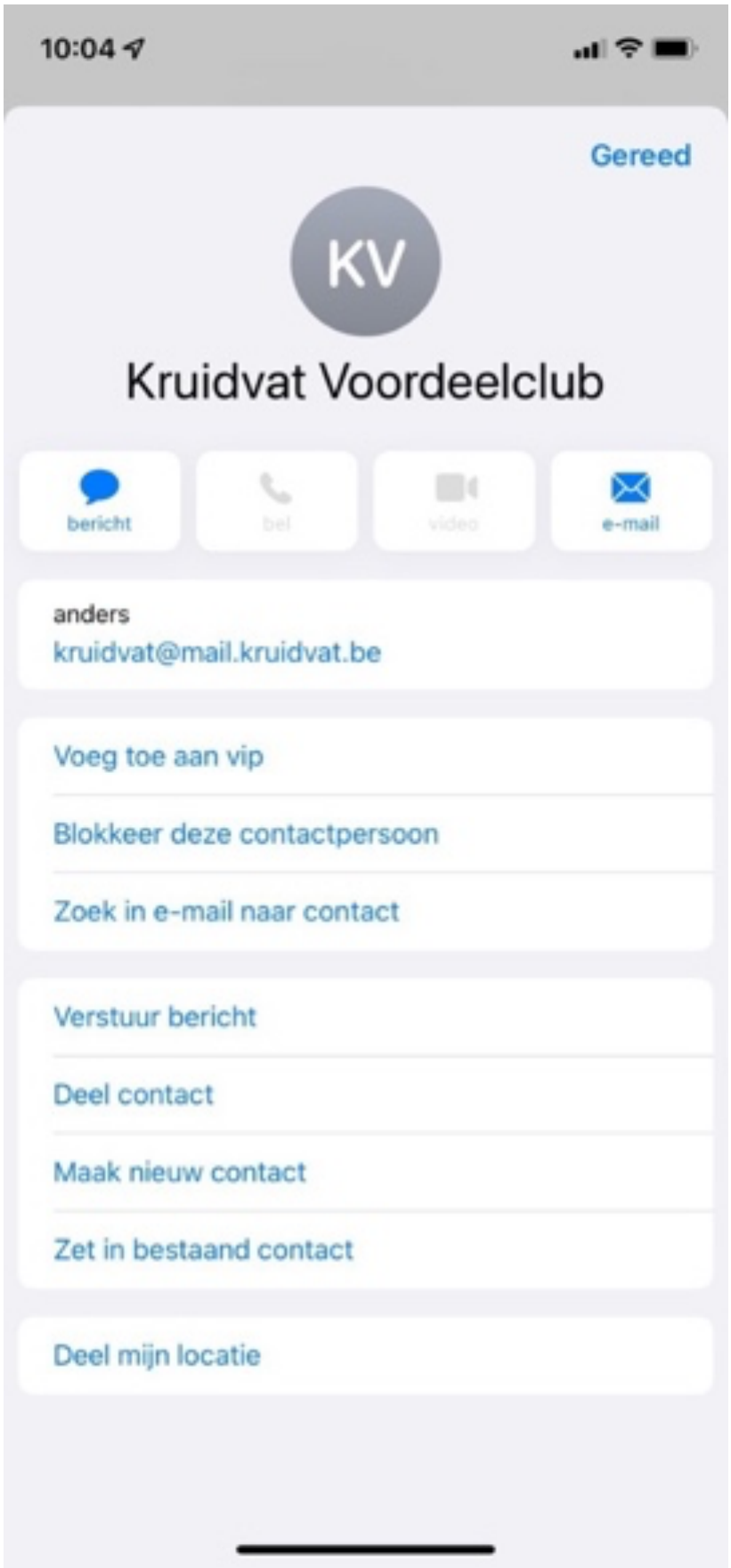
2. Smartphoto



3. Yves Rocher


10:06
Gereed
YB
Yves Rocher België
bericht
bel
video
e-mail
anders
yvesrocher@nl.yves-rocher.be
Voeg toe aan vip
Blokkeer deze contactpersoon
Zoek in e-mail naar contact
Verstuur bericht
Deel contact
Maak nieuw contact
Zet in bestaand contact
Deel mijn locatie

4. Kruidvat


10:04
Gereed
KV
Kruidvat Voordeelclub
bericht
bel
video
e-mail
anders
kruidvat@mail.kruidvat.be
Voeg toe aan vip
Blokkeer deze contactpersoon
Zoek in e-mail naar contact
Verstuur bericht
Deel contact
Maak nieuw contact
Zet in bestaand contact
Deel mijn locatie

9.1.5 Bijlage 5: Steekkaart met tips rond phishing

Tips om phishing te voorkomen

SMS & TELEFOON

- Klik nooit op een link
- Vertrouw geen sms'en van mensen die je niet kent
- Check de landcode: **België = +32, Nederland = +31**
- Geef nooit gegevens door die je niet tegen een vreemde zou vertellen

EMAIL

- Klik niet zomaar op linkjes!
- Geef nooit persoonlijke gegevens door als een e-mail daar om vraagt
- Bekijk het e-mailadres om te zien of het een betrouwbare afzender is
- Bekijk het e-mailadres om te zien of het een betrouwbare afzender is

Tips voor een goed wachtwoord

- Gebruik **geen** opeenvolgende cijfers in een wachtwoord, zoals **123**
- Probeer een **combinatie te maken van kleine letters, grote letters, cijfers en leestekens** zoals een vraagteken of uitroepteken.

Handige website

- ***WWW.MEDIAWIJSHEID.NL***
- ***WWW.CHECKJELINKJE.NL***
- ***WWW.SAFEONWEB.BE***

9.1.6 Bijlage 6: Wachtwoordpuzzel

Eekhoorn	185
123	!
Eend	987
.	eekhoorn
7	eend

9.1.7 Bijlage 7: optioneel deel phishing via websites

Jullie hebben daarnet al bij de andere begeleiders wat geleerd over phishing via telefoon, email en sms. Naast deze drie zijn er nog enkele manieren waarop er soms aan phishing gedaan wordt. We gaan hier nog enkele manieren bespreken. **Hebben jullie een idee welke?**

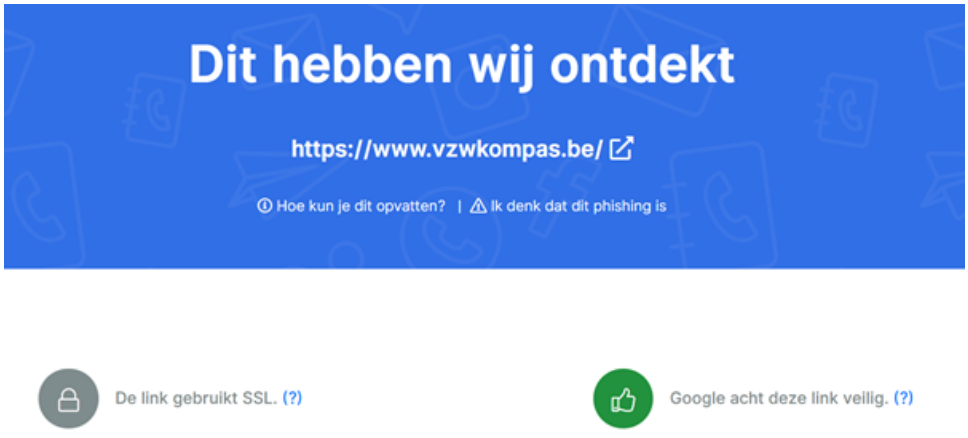
Sommige websites lijken op andere websites, maar blijken in werkelijkheid niet de websites te zijn die je denkt te bezoeken.

Mensen met slechte bedoelingen hebben vaak goed nagedacht op welke manier ze te werk willen gaan. Zo gebeurt het soms dat men websites nabouwt die heel erg op de originele website lijken. Om niet te diep in te gaan op alles hierrond zal ik jullie een manier tonen om verdachte websites te controleren.

Check je link

Via de Nederlandse website https://checkjelinkje.nl/ kan je controleren of een website betrouwbaar is. Dit is niet altijd helemaal correct, maar het geeft je telkens een idee. Indien je twijfelt of een website betrouwbaar is dan is het belangrijk om dit eens na te vragen bij een ouder, begeleider, vertrouwenspersoon.

Bij het controleren van de website van vzw Kompas krijgen we bijvoorbeeld te zien dat volgens hen het lijkt alsof de website van vzw Kompas **veilig** is en dus gewoon gebruikt kan worden.



Controleer de domeinnaam

Heeft iemand van jullie al gehoord van een **domeinnaam?** Als dat niet zo is, geen enkel probleem, ik ga er het belangrijkste van uitleggen.

Elke website die bestaat eindigt op een **punt** gevolgd door 2 of meer letters. Zo eindigt de website van **vzw Kompas** bijvoorbeeld op **.be** zoals je hier kan zien:

https://www.vzwkompas.**be**

Iemand een idee waarvoor die .be zou kunnen staan en waar dit het meest gebruikt wordt?

Bijna ieder land heeft zijn eigen code, daarnaast zijn er nog enkele codes die door verschillende landen samen gebruikt worden. De meest bekende hiervan is **.COM.**

Deze codes zijn een belangrijk onderdeel van wat we **domeinnamen** noemen. Je moet deze codes zeker niet uit het hoofd kennen, dat kan ik ook niet. Maar in sommige gevallen zijn ze belangrijk. Zo zijn er domeinnamen die minder gebruikt worden en die soms een belletje moeten doen rinkelen. Zo worden soms de domeinnamen **.org** en **.net** gebruikt. Dit zijn domeinnamen die goedkoper zijn en kunnen gebruikt worden door mensen met slechte bedoelingen om websites na te bouwen. Door te letten op de domeinnaam kunnen we soms al veel zien.

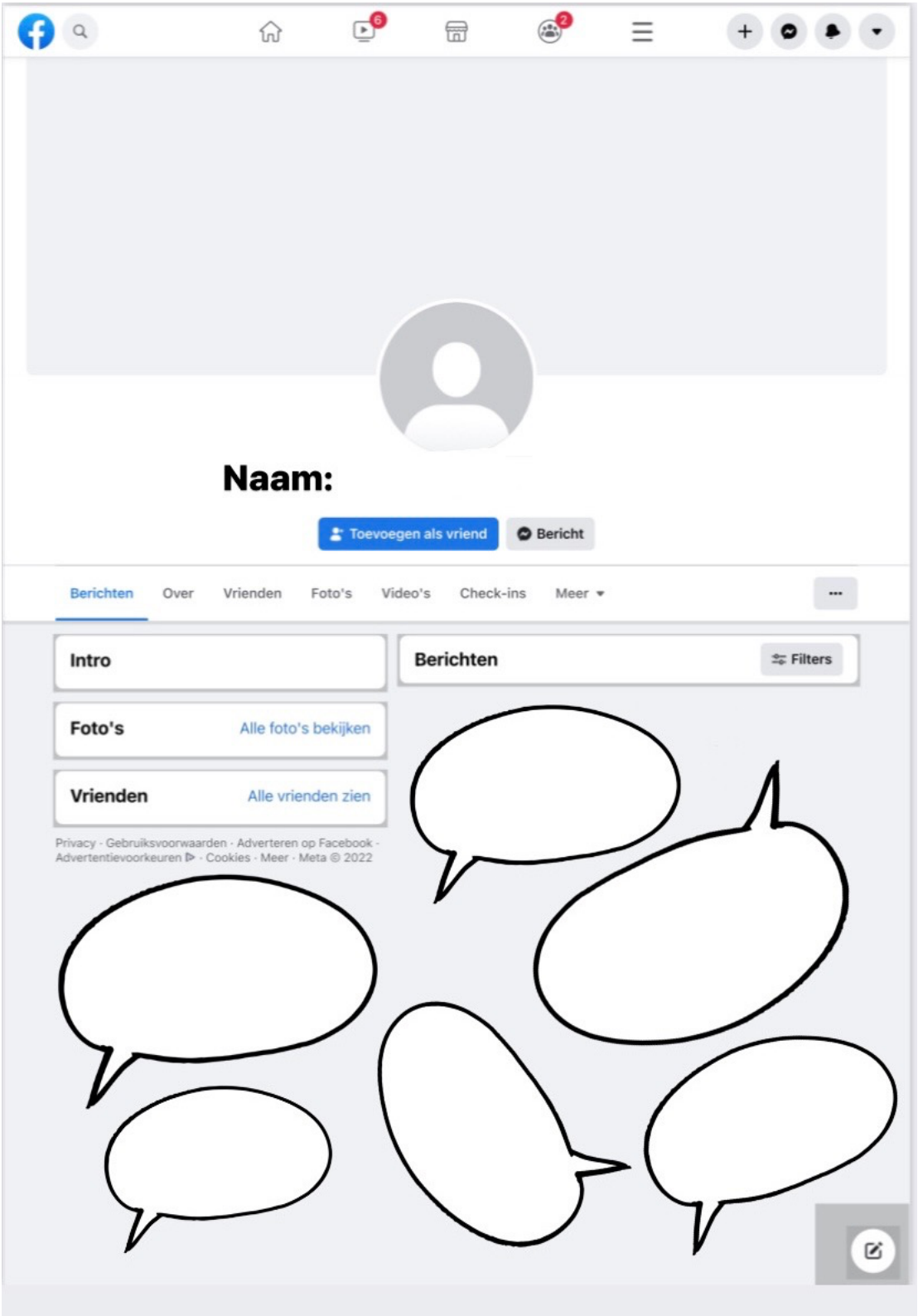
Zo zal bijvoorbeeld een Belgisch bedrijf eerder de code van het land nemen dan bijvoorbeeld **.org** of **.net**

Als we bijvoorbeeld de website van de Belgische post nemen, namelijk WWW.BPOST.BE dan kan je zien dat deze eindigt op **.BE**

Als deze website bijvoorbeeld www.bpost.net zou zijn, dan vraag je dit best eens na bij iemand die je kent. Indien je uiteindelijk toch nog zou twijfelen of je wil helemaal zeker zijn dan **kan je altijd eens bellen** naar het bedrijf of winkel om te controleren of de website klopt.

9.2 Cyberpesten

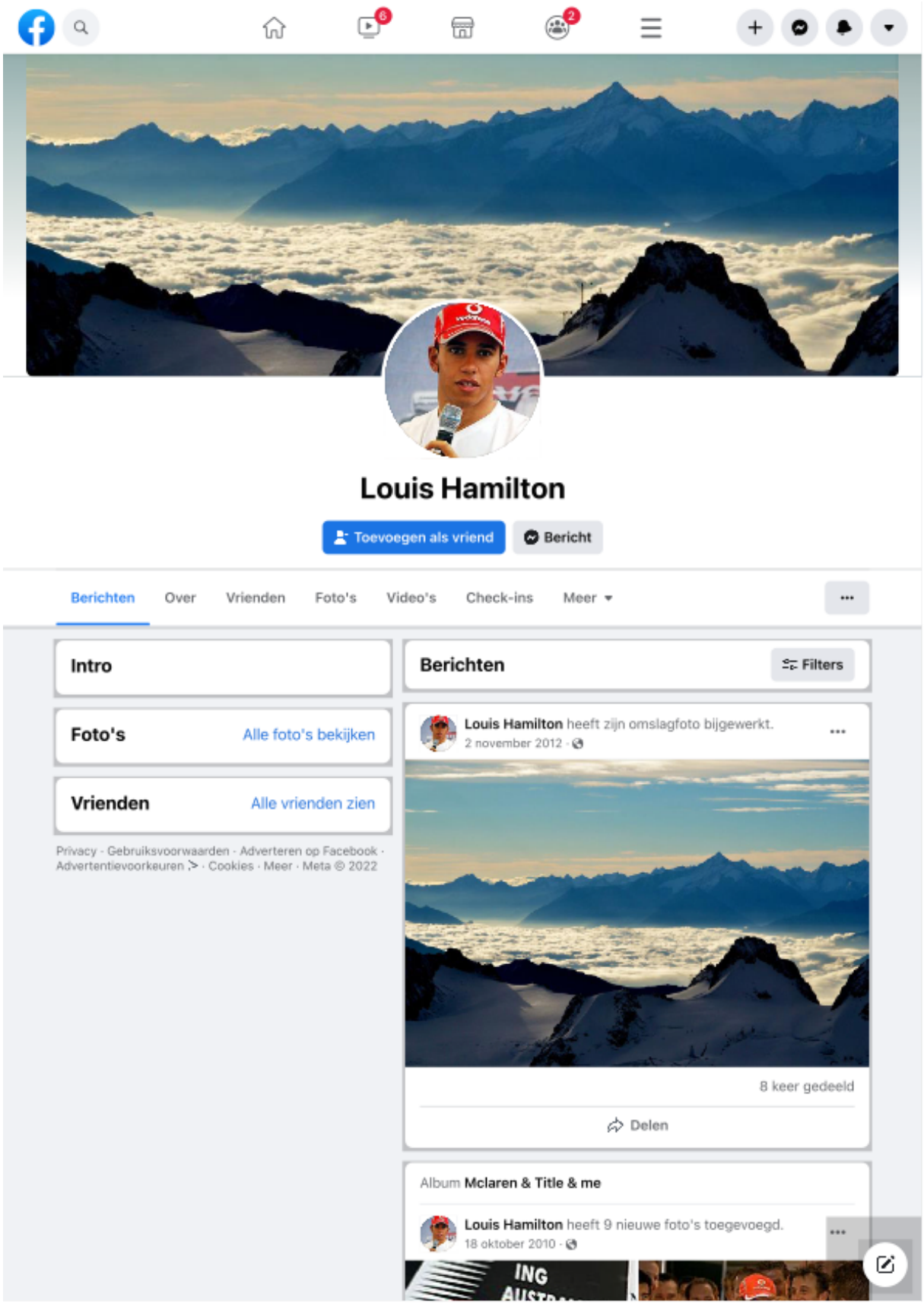
9.2.2 Bijlage: Profiel

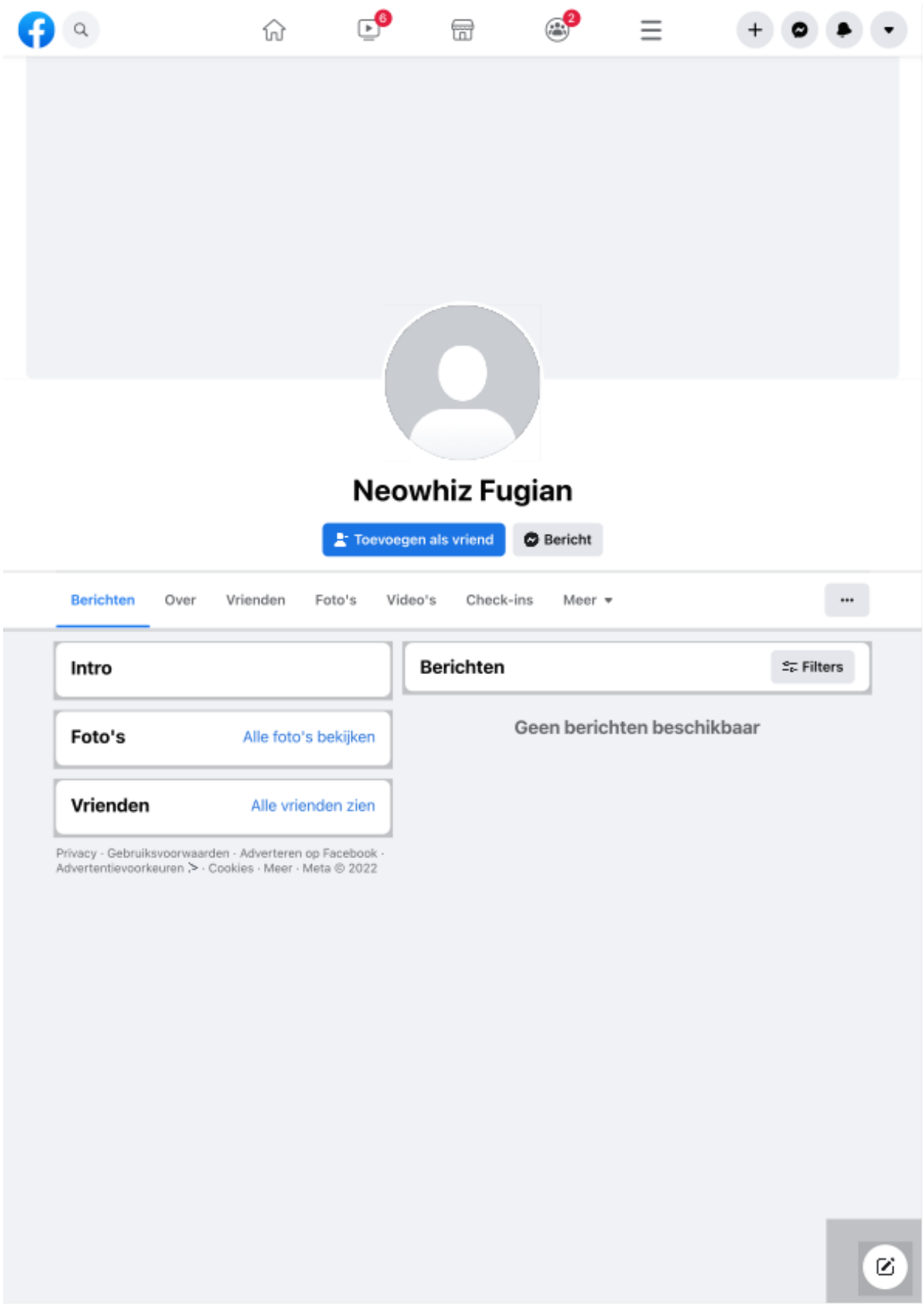


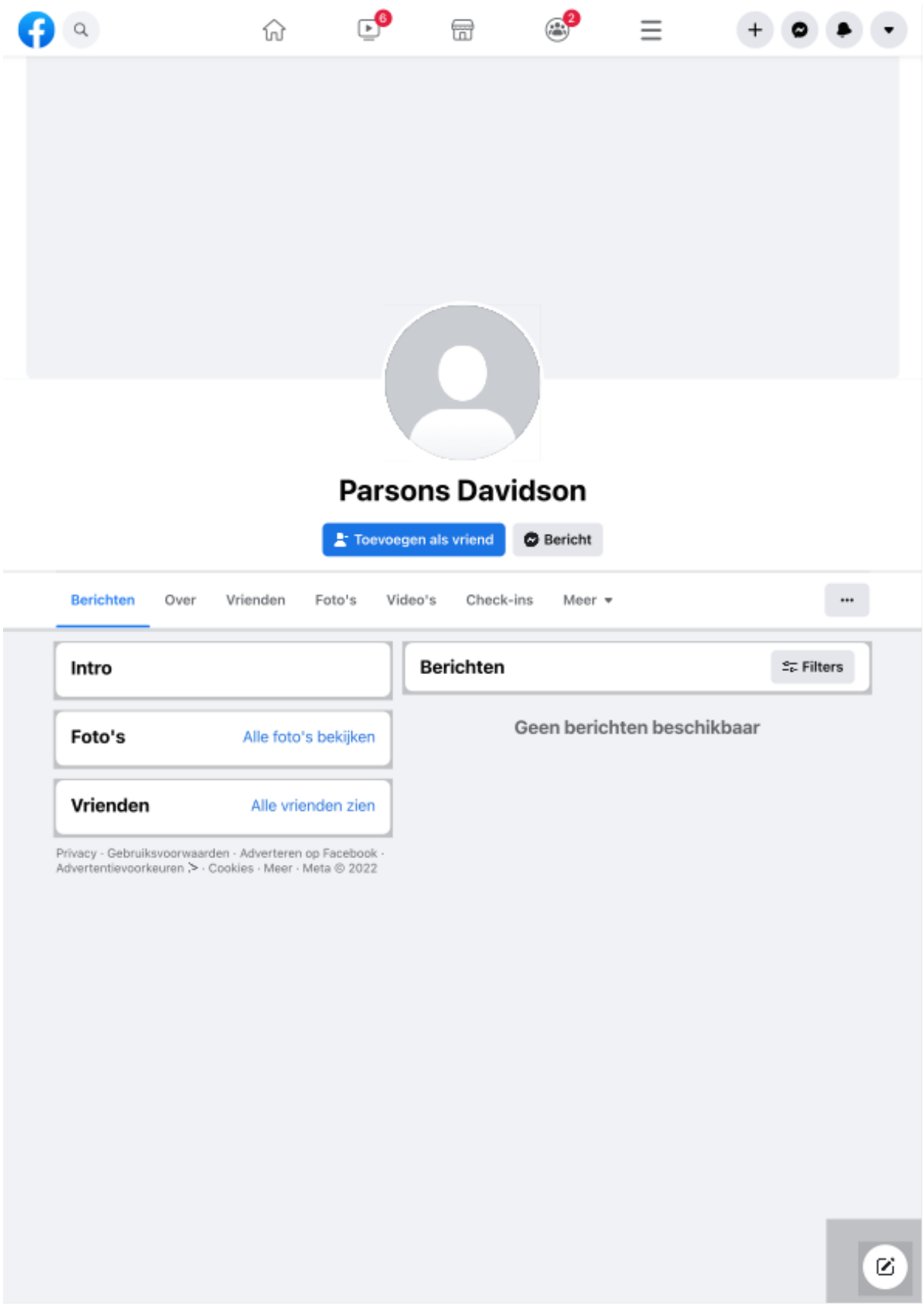
9.3 Nepvrienden

9.3.1 Bijlage: Tipkaart nepvrienden

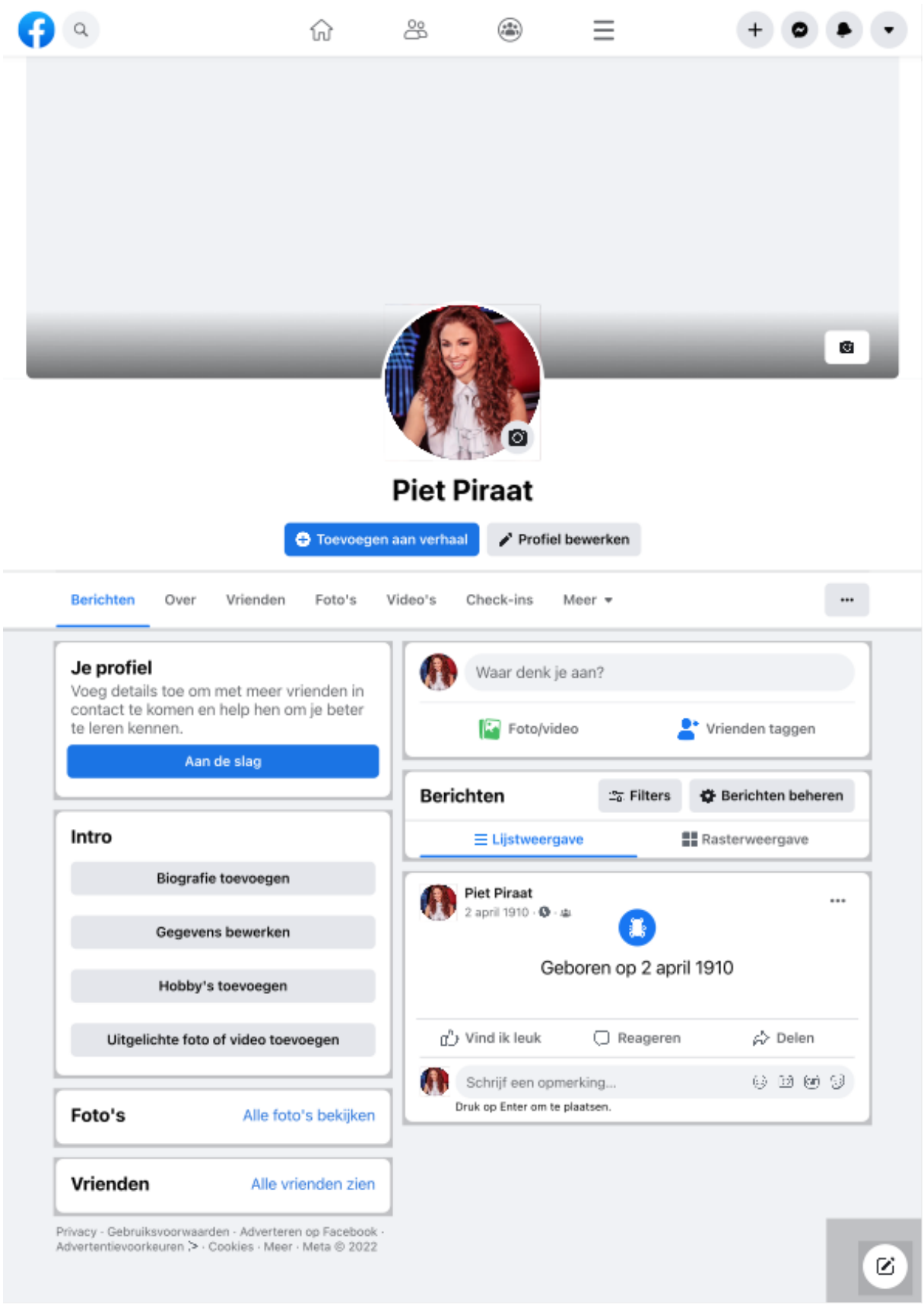
9.3.2 Bijlage 2: voorbeelden fake-profielen




Neowhiz Fugian
Toevoegen als vriend
Bericht
Berichten
Over
Vrienden
Foto's
Video's
Check-ins
Meer
Intro
Foto's
Alle foto's bekijken
Vrienden
Alle vrienden zien
Privacy · Gebruiksvoorwaarden · Adverteren op Facebook · Advertentievoorkeuren · Cookies · Meer · Meta © 2022
Berichten
Filters
Geen berichten beschikbaar



Maryline Verstraeten-Nausch, Jonas Zwaenepoel en Emma Pattyn
Arteveldehogeschool - 2022



Maryline Verstraeten-Nausch, Jonas Zwaenepoel en Emma Pattyn
Arteveldehogeschool - 2022

9.3.3 Bijlage 3: bestaande facebookprofielen