SAXION
UNIVERSITY OF APPLIED SCIENCES

Cyberweerbaarheid

Resultaten van studentonderzoek naar het vergroten van de weerbaarheid van diverse doelgroepen tegen verschillende vormen van cybercriminaliteit.

Lectoraat Maatschappelijke Veiligheid i.s.m.
minor De Digitale Revolutie

Auteurs:
dr. R. (Remco) Spithoven,
dr. Y. (Ynze) van Houten &
M. (Michelle) Walther MSc

Met medewerking van:
mr. B. (Ben) Den Tuinder,
mr. M. (Mark) Dorenbusch,
mr. C. (Christine) Vording &
minorstudenten
De Digitale Revolutie

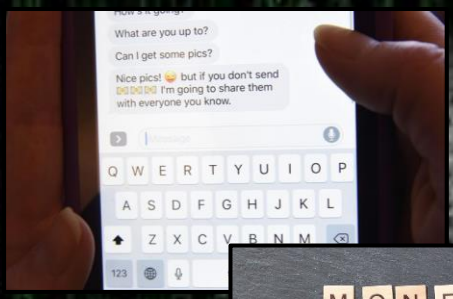
Lectoraat Maatschappelijke Veiligheid, Hogeschool Saxion
2020

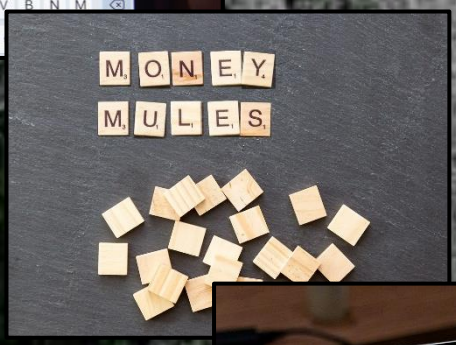
Cybercriminaliteit ontvangt de laatste jaren steeds meer maatschappelijke aandacht. En terecht. Waar de offline criminaliteit in de politieregistraties en slachtofferenquêtes een dalende trend laat zien vanaf 2000, zien wij vanaf 2012 – het jaar waarin we slachtofferschap van cybercriminaliteit zijn gaan meten – een groeiend online slachtofferschap.

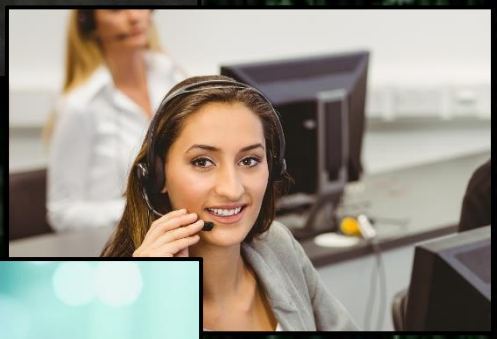
Naar schatting wordt één op de acht burgers en zelfs één op de vijf mkb-bedrijven jaarlijks het slachtoffer van cybercriminaliteit. Offline zetten we nog de meest waardeloze fiets op een dubbel slot, maar online laten we onze deuren en ramen wagenwijd openstaan. Daar moet verandering in komen. Maar hoe?

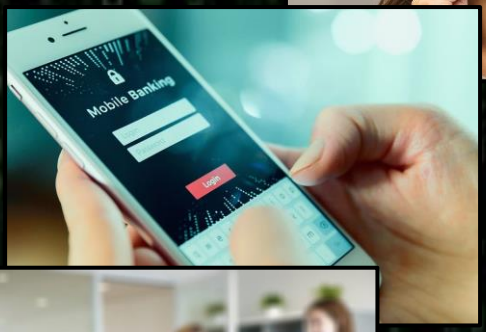
Een multidisciplinaire groep studenten van de Saxion-minor De Digitale Revolutie deed in samenwerking met het lectoraat Maatschappelijke Veiligheid onderzoek naar dit urgente vraagstuk. Een goede opwarmer voor hun afstuderen met mooie resultaten! In deze publicatie brengen wij verslag uit van onze bevindingen.

dr. Remco Spithoven
Lector Maatschappelijke Veiligheid, Saxion

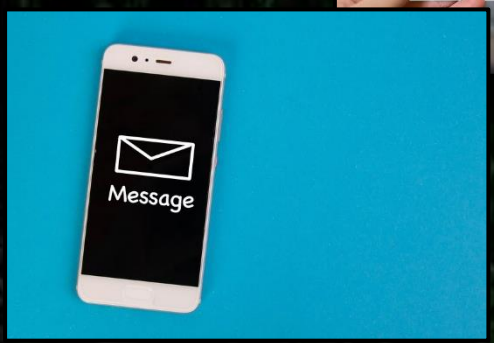

What are you up to?
Can I get some pics?
Nice pics! but if you don't send I'm going to share them with everyone you know.

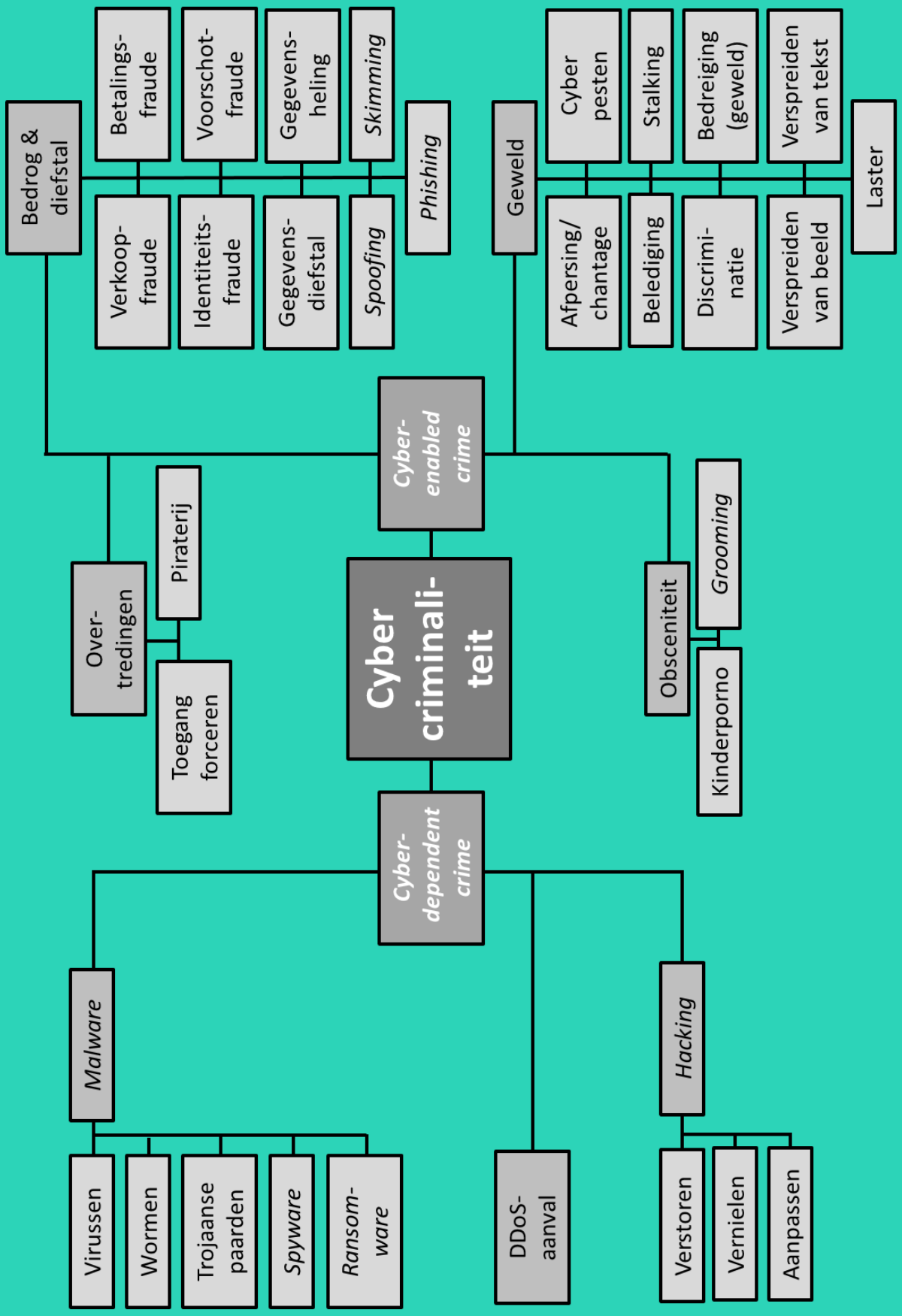

MONEY
MULES




Mobile Banking
Login


WE'RE
HIRING


Message



Figuur 1 – Taxonomie van cybercriminaliteit (Spithoven 2020, p. 49).

Uitgangspunten & conclusies

dr. Remco Spithoven
dr. Ynze van Houten
Michelle Walther MSc

Cybercriminaliteit "Het gebruiken van het internet of andere informatietechnologie ten behoeve van het faciliteren van criminaliteit of ander norm-overschrijdend gedrag" (Spithoven, 2020, p. 121 op basis van Kleve, de Mulder & Van Noortwijk, 2010; Holt & Bossler, 2014; Leukfeldt, 2016).

Cyberweerbaarheid "Weerbaarheid van eindgebruikers van informatietechnologie tegen cybercriminaliteit op basis van risicobewustzijn en zelfbeschermend gedrag" (Spithoven, 2020. p. 59).

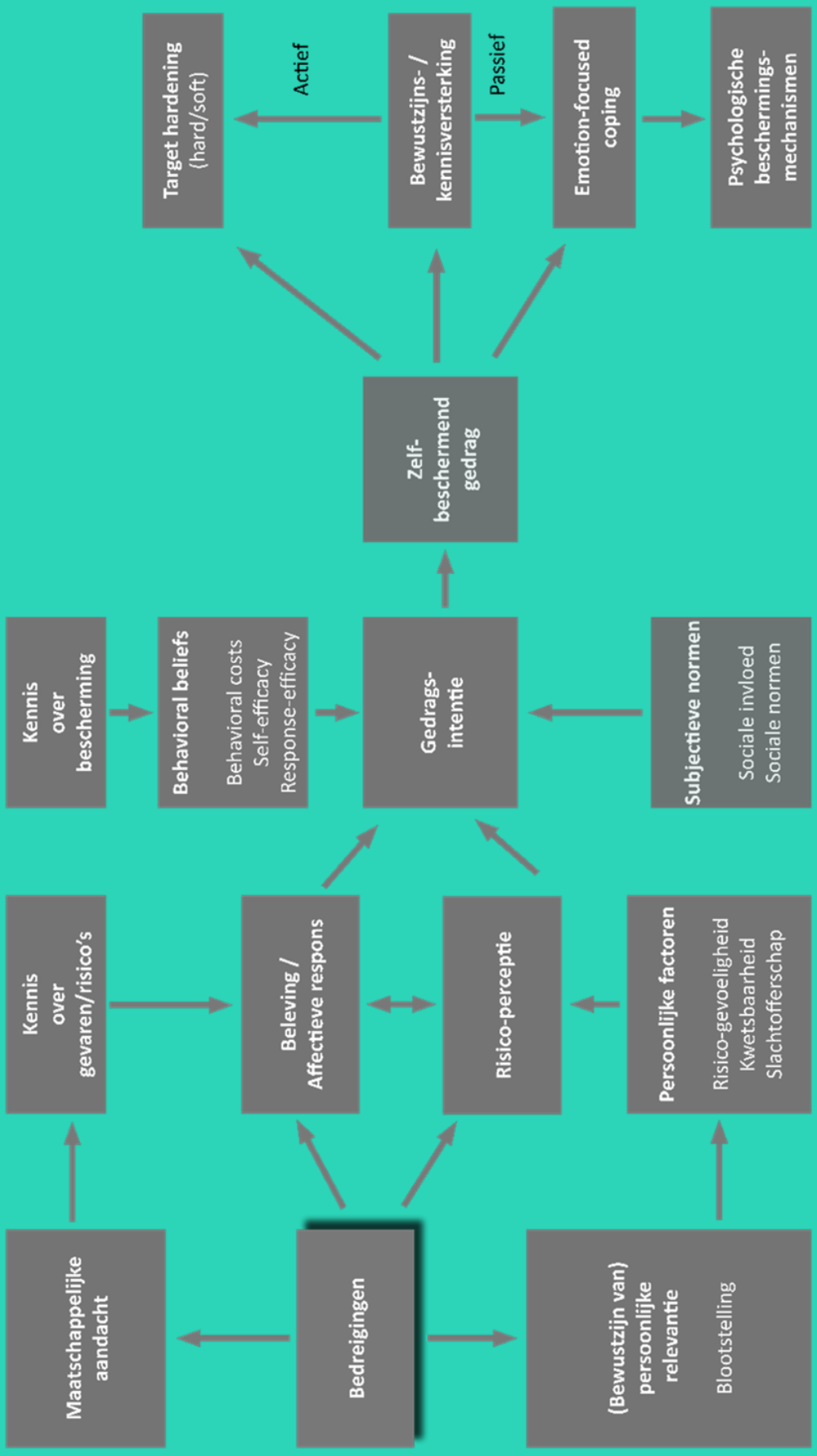
De offline criminaliteit is niet *out of the blue* gedaald. De internationale crimedrop is het gevolg van een toegenomen mate van beveiliging in de Westerse samenlevingen, zo concluderen criminologen (De Jong, 2018; Farrell et al., 2011; 2014; Van Dijk, Tseloni & Farrell, 2012).Onder deze toegenomen beveiliging ligt logischerwijs: (I) een toegenomen maatschappelijk bewustzijn, (II) de overtuiging dat het eigen gedrag en de eigen maatregelen effect hebben op de kans op slachtofferschap, (III) een bereidheid in maatregelen te investeren of eigen gedrag aan te passen, en (IV) de mogelijkheid om maatregelen te treffen of het eigen gedrag aan te passen.

In dit onderzoek staat de vraag 'Hoe kunnen specifieke doelgroepen meer cyberweerbaar worden?' centraal. Elke studentengroep richtte zich op een andere doelgroep en een andere specifieke vorm van cybercriminaliteit. Waarom? Omdat cyberweerbaarheid maatwerk is!

Niet elke vorm van cybercriminaliteit is namelijk hetzelfde. We onderscheiden twee categorieën. Onder (I) *cyber-enabled criminaliteit* worden meer klassieke vormen van criminaliteit verstaan die door middel van ICT op een grotere schaal kunnen worden uitgevoerd, zoals oplichting, identiteitsfraude en phishing. Naast gedigitaliseerde, klassieke criminaliteit is er ook sprake van compleet nieuwe vormen van criminaliteit die zonder de nieuwe ICT onmogelijk zou zijn. Onder deze nieuwe vormen van (II) *cyber-dependent crime* wordt criminaliteit verstaan die wordt gepleegd door middel van ICT met ICT als doelwit, zoals bijvoorbeeld hacken, DDoS-aanvallen, virussen, ransomware en andere malware.

Inmiddels is cybercriminaliteit een veelkoppig monster, zoals in de taxonomie van Spithoven in Figuur 1 goed is te zien. Elke vorm van cybercriminaliteit kent zijn eigen wegen waarlangs het ontstaat, maar duidelijk is dat voor het gros van de cybercriminaliteit de mens de zwakste schakel vormt. We moeten dus naast een specifieke focus op cyberdelicten ook oog hebben voor het feit dat ieder mens uniek is en daarom risico's anders zal beleven, en zijn of haar gedrag niet zomaar aan zal passen. In Figuur 2 is het theoretisch model opgenomen dat onderzoekers van het lectoraat Maatschappelijke Veiligheid ontwikkelde om inzicht te geven in de factoren en processen die zelfbeschermend gedrag beïnvloeden..

We leggen dit theoretische model nu op hoofdlijnen uit. De individuele doelstelling om zelfbeschermend gedrag te vertonen in het nemen van maatregelen of het aanpassen van het eigen gedrag ontstaat onder invloed van verschillende factoren. Ten eerste is er de beleving van de risico-perceptie en de beleving (of de affectieve respons) die deze dreiging teweeg brengt. Deze twee factoren staan op hun beurt onder invloed van de kennis die het individu van het risico heeft en de maatschappelijke aandacht die het risico heeft ontvangen. Gezamenlijk leiden deze factoren tot een inschatting hoe relevant het risico voor het individu is. Dit wordt medebepaald door persoonlijke kenmerken zoals de risicogevoeligheid en de ingeschatte kwetsbaarheid van het individu.



Figuur 2 – Theoretisch model cyberweerbaarheid (Spithoven, 2020).

Ook is van invloed in welke mate een individu denkt dat anderen verwachten dat hij zichzelf tegen het risico te beschermen en in hoeverre deze persoon geneigd is hieraan te voldoen (dit noemen we de subjectieve normen) en dat het individu ervan overtuigd is dat het zelfbeschermend gedrag tot het gewenste effect zal leiden (dit noemen we de *behavioral beliefs*). Het doel is uiteindelijk dat het individu het eigen gedrag aanpast of beschermende maatregelen treft, om zo een minder geschikt doelwit te worden van cybercriminalitet (*target hardening*).

Toch is dit erg lastig, want mensen zijn niet zomaar overtuigd van het feit dat zij zelf risico lopen. Dit komt doordat mensen zijn geprogrammeerd om negatieve emoties en gedachten te neutraliseren. Vaak treedt daarom op wat we *emotion-focused coping* noemen: we negeren het risico door alleen iets aan de gedachte of het gevoel te doen. We gaan wat anders doen ter afleiding, of ons eigen onderbewuste neutraliseert de gedachten en gevoelens door bijvoorbeeld het risico in onze gedachten te verschuiven naar kwetsbaardere mensen. We noemen deze dynamieken – zoals de ontdekker Sigmund Freud ze ook noemde – 'psychologische beschermingsmechanismen'.

Met deze theoretische bagage stelden we de multidisciplinaire studentengroepen de vraag welke doelgroep en welk type cybercriminaliteit zij het interessantst zouden vinden om onderzoek naar te doen Het onderzoek moest de risicoperceptie en het zelfbeschermende gedrag van de gekozen doelgroep in kaart brengen, en aangeven met welke interventies de cyberweerbaarheid van de groep kan worden vergroot. Al snel waren de keuzes helder en beargumenteerden de groepen waarom zij de keuzes maakten voor… :

I. … shame sexting & sextortion onder scholieren;
II. … money muling onder mbo-studenten;
III. … ransomware onder mkb'ers;
IV. … helpdeskfraude onder ouderen;
V. … vacaturefraude onder werkzoekenden;
VI. … tikkiefraude onder young professionals;
VII. … smishing onder senioren.

De studentengroepen hebben gedreven aan hun onderzoeken gewerkt. Tussentijds hebben wij de voortgang afgestemd en waren wij beschikbaar voor eventuele vragen. Dankzij de inzet van de studenten kunnen we de volgende overkoepelende conclusies trekken:

I. Respondenten zijn nog **vrij onbekend met de onderzochte vormen van cybercriminaliteit**. Na enige toelichting door de studenten gaat er wel wat dagen en hadden zij wel een algemeen idee van de risico's, maar dit werd maar zelden als persoonlijk relevant ervaren;
II. Er is duidelijk sprake van een ***optimistic bias*** onder de respondenten. Men ziet de relevantie van het risico voor de algemene groep waartoe men behoort, maar heeft het idee zelf een klein risico te lopen;
III. Er is nog **veel winst te behalen in het risicoperceptie en zelfbeschermend gedrag** ten aanzien van de meeste vormen van cybercriminaliteit;
IV. Er wordt **veel invloed van voorlichting verwacht**, per doelgroep wordt daarbij op andere communicatiekanalen ingespeeld.
V. Het bevorderen van **cyberweerbaarheid is maatwerk**.

Deze overkoepelende resultaten zijn in lijn met de resultaten van ons eerdere onderzoek naar cyberweerbaarheid dat wij samen met het lectoraat cybersecurity in het mkb van de Haagse Hogeschool deden en waarop dit studentenonderzoek is gestoeld. De komende jaren zullen wij samen met hen, het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, vier regionale samenwerkings-verbanden en twaalf gemeenten toegepast wetenschappelijk onderzoek naar het vergroten van de cyberweerbaarheid van verschillende doelgroepen verrichten vanuit onze onderzoekslijn Digitale Weerbaarheid. Ook in dat project trekken we graag weer met studenten op en we zien uit naar de volgende lichting van deze minor!


Remco Spithoven


Ynze van Houten


Michelle Walther

Hey.

How's it going?

What are you up to?

Can I get some pics?

Nice pics! 😜 but if you don't send 💵💵💵 I'm going to share them with everyone you know.

iMessage

Q W E R T Y U

A S D F G H J

Z X C V B N

Shame sexting & Sextortion

Diede Meijer (Integrale Veiligheidskunde)
Dominic Wessels (Security Management)
Daan te Wierik (Security Management)
Esmee van 't Hoog (HBO Rechten)
Bahara Parwana (HBO Rechten)

Shame sexting "Shame-sexting is het zonder toestemming maken en/of verspreiden van naaktbeelden of seksfilmpjes" (Schoolenveiligheid.nl, *z.d.*).

Sextortion "Naaktbeelden gebruiken als chantage- en dwangmiddel om geld los te krijgen of het slachtoffer seksuele handelingen te laten verrichten." (Schoolenveiligheid.nl, *z.d.*).

Wat hebben jullie onderzocht?

In hoeverre jongeren (12-24 jaar) in de regio Twente zich bewust zijn van shame sexting en sextortion en hoe groot zij de kans op slachtofferschap inschatten.

Waarom hebben jullie dit onderzocht?

Het afpersen door middel van intieme beelden is volgens ons een probleem omdat het leven van jongeren zich steeds meer online afspeelt. Ook zijn jongeren op die leeftijd zich vaak niet of nauwelijks bewust van de risico's die het versturen van intieme beelden met zich meebrengt. Verder is de instapdrempel erg laag en zijn er relatief makkelijk en veel potentiële slachtoffers te vinden.

Hoe hebben jullie dit onderzocht?

Om kennis te verkrijgen over het onderwerp hebben wij allereerst een literatuuronderzoek uitgevoerd. Hierbij is gebruik gemaakt van verschillende bronnen. Zo zijn internetbronnen gebruikt die zijn geschreven door deskundigen, maar ook nieuwsartikelen die (historische) gebeurtenissen toelichten en algemene cijfers verschaffen.

Om de risicoperceptie van shame sexting en sextortion onder jongeren (12-24 jaar) in de regio Twente te meten is gebruik gemaakt van kwantitatief onderzoek. Hiervoor hebben we in nauwe afstemming met het lectoraat Maatschappelijke Veiligheid een vragenlijst ontwikkeld. Deze is ingevuld door 179 jongeren bij een opleidingsinstituut binnen de regio Twente. Zij zijn voorafgaand door ons en hun opleiding geïnformeerd over het doel van het onderzoek en deelname was volledig vrijwillig en anoniem. De leerlingen waren tussen de 12 en 21 jaar. Dit bleek uit ons literatuuronderzoek een erg kwetsbare doelgroep, omdat dit de periode is dat jongeren in hun puberteit zitten en hun leven zich voor een groot gedeelte online afspeelt.

Ook hebben wij verdiepende interviews gehouden met professionals die van verschillende organisaties die te maken kunnen krijgen met slachtoffers van shame sexting en sextortion. Dit waren:

I. Jeugdcoördinator van de veiligheidskamer (voorheen Bureau Halt);
II. Een vertrouwenspersoon bij een opleidingsinstituut;
III. Een jeugdagent;
IV. Een seksuoloog;
V. Een medewerker van de GGD.

Onze vragen aan de professionals hebben we op semi-gestructueerde wijze afgenomen.

Wat waren jullie belangrijkste bevindingen?

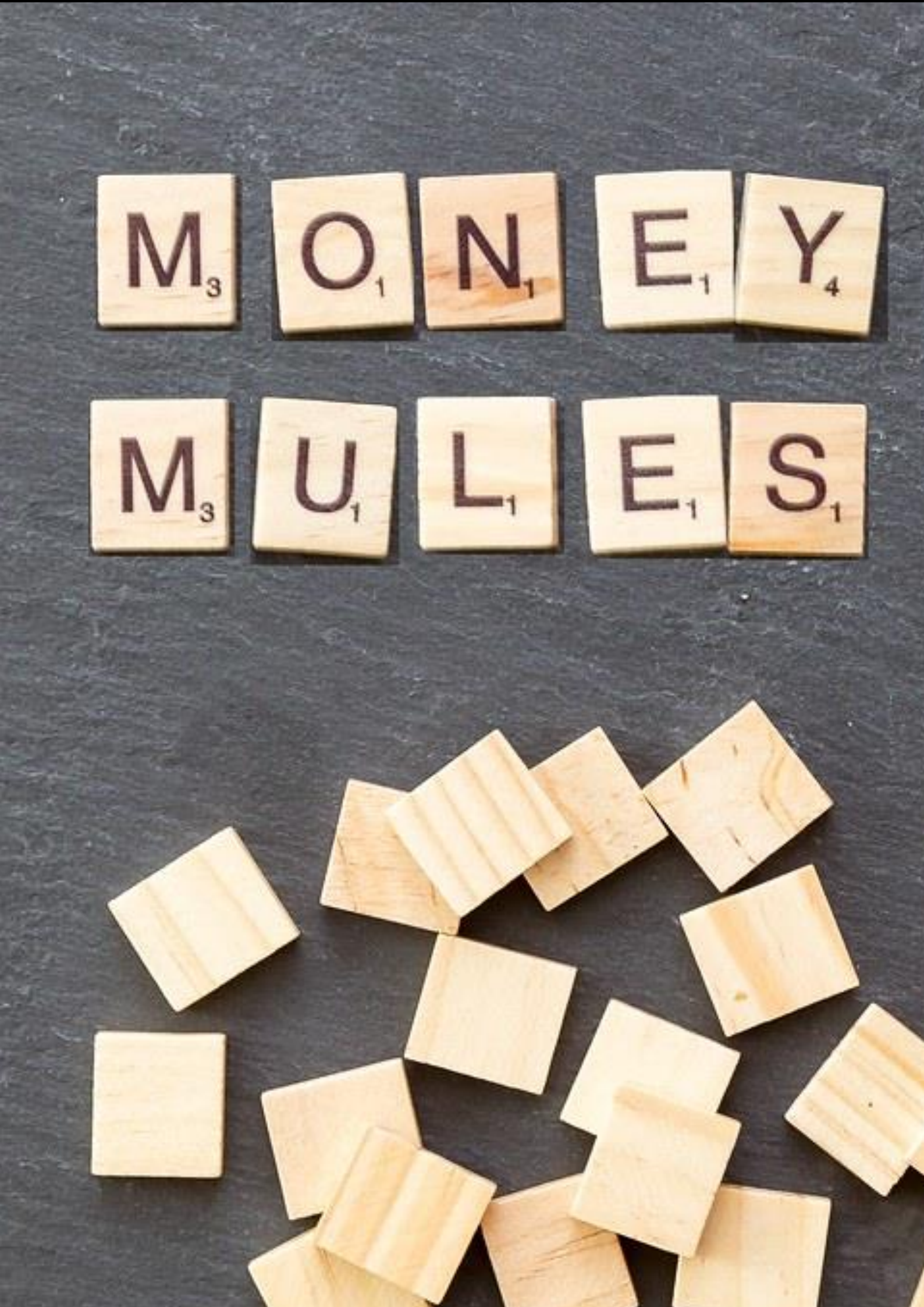
De overgrote meerderheid (83%, n= 149) van de jongeren die onze vragenlijst invulden wist wat sexting is. Maar shame sexting en sextortion waren vrij onbekend onder onze respondenten. Slechts 25% (n=45) gaf aan te weten wat shame sexting is en maar 15% (n=27) wist naar eigen zeggen wat sextortion is. Daarbij viel op dat vrouwelijke deelnemers naar eigen zeggen iets bekender waren met deze fenomenen dan mannelijke respondenten. Wat ook opviel was dat er sprake was van een flinke

optimistic bias onder onze respondenten: 79% (n=142) denkt zelf een hele kleine kans te hebben om slachtoffer van shame sexting of sextortion te worden terwijl 59% (n= 106) een grote tot zeer kans op slachtofferschap voor anderen in dezelfde leeftijd ervaren.

Hoe kan slachtofferschap van shame sexting en sextortion onder jongeren volgens jullie worden tegengegaan?

De risicoperceptie en het preventieve gedrag kan volgens ons aanzienlijk worden verhoogd onder de jongeren als de volgende interventies worden geïmplementeerd:

I. Vroegtijdig in het basisonderwijs en middelbare scholen aanbieden van lessen over cybercrime, waarbij niet alleen wordt ingegaan op sexting, maar ook op andere cybercrimes;
II. Bespreekbaar maken door de ouders. Sexting en seksueel gedrag is een opvoedingszaak. Het is belangrijk dat de ouders het gesprek aan durven te gaan en zelf bekend zijn met de risico's van deze tijd;
III. Actieve vormen van voorlichting. Bijvoorbeeld in de vorm van een escape room of een theatervoorstelling;
IV. Campagnes via social media. Het leven van jongeren speelt zich in grote mate digitaal af. Prikkelende campagnespotjes met influencers zullen een groot effect hebben op de jongeren.


MONEY
MULES

Money mules

Mark Nijhof (Integrale Veiligheidskunde)
Stijn Huijsmans (Security Management)
Robbert Poel (Security Management)
Bart Hendriks (HBO Rechten)

Money mule Een persoon die geld voor een resterende vergoeding door criminelen op de eigen bankrekening laat zetten. Het grootste gedeelte van het geld wordt door middel van pinnen of op andere manier weer aan de criminelen overgedragen (o.b.v. Leukfeldt & Kleemans, 2019).

Wat hebben jullie onderzocht?

De risicoperceptie en het preventief gedrag onder jongvolwassenen (18 t/m 22 jaar) ten aanzien van money muling. Ook hebben we onderzocht hoe de risicoperceptie en het preventieve gedrag kan worden gestimuleerd.

Waarom hebben jullie dit onderzocht?

Het fysiek of digitaal beschikbaar stellen van de eigen bankrekening aan criminelen door jongvolwassenen is een groot probleem in Nederland en kan zware gevolgen hebben voor de money mule (geldezel). De jongeren krijgen op korte termijn een flinke vergoeding voor het beschikbaar stellen van hun rekening, maar zijn zich vaak niet bewust van het feit dat het hierbij gaat om zwart geld dat van misdrijven afkomstig is. Met het beschikbaar stellen van hun bankrekening zijn zij medeplichtig aan witwassen. Dit is strafbaar en kan langdurige, negatieve gevolgen voor de money mule hebben.

Hoe hebben jullie dit onderzocht?

Allereerst hebben we op basis van deskresearch in kaart gebracht hoe de doelgroep te kenmerken is. Hieruit bleek, dat de belangrijkste doelgroep bestaat uit jongeren van 18 tot 22 jaar. Om de risicoperceptie en het preventief gedrag van de doelgroep te meten hebben wij gebruik gemaakt van kwalitatief onderzoek in de vorm van diepte-interviews. Deze interviews werden gehouden met twaalf leerlingen van verschillende opleidingen in Utrecht. Ook hebben wij een voorlichtingsbijeenkomst van de Politieacademie op een school in Apeldoorn bezocht om te zien hoe de huidige voorlichtingscampagnes eruit zien.

Wat waren jullie belangrijkste bevindingen?

De respondenten waren over het algemeen niet bekend met de term money mule. Ook waren ze zich (bijna) niet bewust van het risico dat money muling voor hunzelf en de samenleving kan vormen, Slechts vier respondenten hadden een vaag idee van het risico. Wanneer later in het interview de term geldezel werd gebruikt bleek dat deze term vaker bekend was.

Over de mogelijke gevolgen van het ingaan op een verzoek om de bankrekening beschikbaar te stellen aan een ronselaar tastten al onze respondenten in het duister. De ene helft vond na uitleg dat money muling een maatschappelijk probleem is, de andere helft zag het probleem er niet van in. Toch kwam het wel in hun omgeving voor. Een respondent gaf aan dat iemand in de familie een money mule is geweest en vier respondenten gaven aan dat vrienden dat ooit waren.

Wanneer zij zelf door een ronselaar benaderd zouden worden, zouden nagenoeg alle respondenten er met vrienden over praten. Driekwart zou er met familie over praten. De respondenten wisten ook niet goed wat de gevolgen kunnen zijn. Meerdere respondenten gaven aan dat ze graag zouden willen weten wat de eventuele gevolgen zijn als zij money mule zijn. Meerdere respondenten hebben het idee dat zij niet tot de doelgroep behoren en dat ze minder snel zouden ingaan op een ronselaar dan anderen.

Hoe kan money muling onder jongeren volgens jullie worden tegengegaan?

De risicoperceptie en het preventieve gedrag onder jongvolwassenen kan volgens ons worden verhoogd door:

I. Gerichte reclame op sociale media en televisie te verspreiden waarbij zowel de jongvolwassenen (social media) als de ouders (televisie) te bereiken zijn. Verder is het belangrijk om gesprekken tussen jongvolwassenen en hun ouders over dit onderwerp te stimuleren.
II. Voorlichtingen via tastbare praktijkvoorbeelden op scholen te houden en op verhalen van ervaringsdeskundigen/ex-geldezels inzetten om de doelgroep bewust te maken van de risico's van money muling.

Ransomware

Stijn Haandrikman (Security Management)
Ruben van Loon (Security Management)
Stan Hulsegge (Bestuurskunde)
Ronald Huisjes (HBO Rechten)

Ransomeware ‘Schadelijke gijzelsoftware die schade aan bestanden en netwerken toebrengt door gegevens te versleutelen of te blokkeren en tegen betaling te herstellen’ (Spithoven 2020, p. 52, o.b.v. Holt & Bossler, 2014; Leukfeldt, 2016; CBS, 2018; Holt, Bossler & Seigfried-Spellar, 2018).

Wat hebben jullie onderzocht?

We hebben allereerst gekeken welke juridische instrumenten er bestaan om het gebruik van ransomware door cybercriminelen tegen te gaan. Daarnaast hebben we onderzocht met welke maatregelen de ondernemers in het midden- en klein bedrijf zich op dit moment tegen ransomware beschermen en hoe zij worden geholpen zichzelf beter te beschermen. Ook hebben we onderzocht hoe de risicoperceptie van mkb’ers ten aanzien van ransomware is en hoe zij dit risico in hun eigen bedrijf verkleinen.

Waarom hebben jullie dit onderzocht?

De aandacht voor ransomware groeit en heeft vaak financiële consequenties voor het slachtoffer. Een recent voorbeeld hiervan is het platleggen van het netwerk van de Universiteit Maastricht door cybercriminelen door middel van ransomware. Voor het ontsleutelen heeft de Universiteit Maastricht maar liefst € 200.000,- moeten betalen. Ransomware lijkt steeds vaker gericht te worden ingezet en dus op een specifiek doelwit ingezet te worden in plaats van de ransomware algemeen te verspreiden.

Hoe hebben jullie dit onderzocht?

Om kennis op te doen over ransomware hebben wij gebruik gemaakt van literatuur uit wetenschappelijke en andere (openbare) bronnen om. Om de risicoperceptie van de mkb'ers en hun zelfbeschermend gedrag te meten, hebben wij kwalitatief onderzoek uitgevoerd. Hiervoor zijn er tien semigestructureerde interviews afgenomen met mkb'ers.

Wat waren jullie belangrijkste bevindingen?

De dreiging van ransomware voor mkb'ers is onverminderd hoog en lijkt niet af te nemen. Het strafrecht lijkt niet voldoende preventieve werking te hebben omdat cybercriminelen hun digitale sporen vaak goed maskeren en doorgaans niet gepakt worden. Daarbij lijken zij gerichter slachtoffers te zoeken waarbij de kans op snelle betaling van grote bedragen groter is.

Van de tien ondernemers die zijn geïnterviewd gaven er zes aan niet goed genoeg beveiligd te zijn. Hoewel bij vier ondernemers wel een aantal maatregelen aanwezig is, bieden deze maatregelen onvoldoende bescherming. Eén ondernemer had elke week een IT'er over de vloer die ook ondersteunt in het tegengaan van gelegenheid voor cybercrime.

De ondernemers maken wel regelmatig back-ups maar de opslag van deze backups is vaak aan het bedrijfsnetwerk aangesloten, waardoor ook deze versleuteld kunnen worden. Verder hebben wij gezien dat de ondernemers het risico van ransomware wel kennen, maar de impact van de aanval onderschatten en vaak geen kennis van hun eigen kans op een aanval hebben. De ondernemers die wij interviewden bleken met andere woorden het risico erg laag in te schatten, waardoor zij geen of weinig maatregelen treffen.

Hoe kan slachtofferschap van ransomware onder mkb'ers volgens jullie worden tegengegaan?

De risicoperceptie en het preventieve gedrag ten opzichte van ransomware onder de mkb'ers kan volgens ons aanzienlijk worden verbeterd door:

I. Het ronddelen van flyers en het houden van bijeenkomsten door netwerken waar ondernemers al goed contact mee hebben, bijvoorbeeld mkb-verenigingen;
II. Het aandragen van maatregelen die voor mkb'ers eenvoudig uitvoerbaar, effectief zijn en niet teveel tijd en geld kosten;
III. Het invoeren van de zogenoemde 3-2-1 back-up strategie: deze voorkomt schade van een ransomware-aanval binnen het bedrijf. Deze strategie houdt in: Zorg voor minimaal 3 back ups van je data; zorg ervoor dat 2 backups op verschillende opslagmedia staan en houd er 1 buiten het reguliere bedrijfsnetwerk. Zorg ervoor dat iemand persoonlijk verantwoordelijk is voor het routinematig borgen van deze strategie;
IV. Het installeren van een goede, up-to-date virusscanner die helpt bij het afweren van de meeste standaard vormen van ransomware.

Helpdeskfraude

Femke Goedhart (Integrale Veiligheidskunde)
Maurice Perik (Security Management)
Colin Puhl (Security Management)
Stefan Musch (HBO Rechten)

Helpdeskfraude Helpdeskfraude is een vorm van oplichting waarbij fraudeurs doen alsof ze helpdeskmedewerkers van grote, bekende bedrijven zijn. De oplichters zeggen daarbij doorgaans dat er iets ernstigs met de computer van het slachtoffer aan de hand is. Als het slachtoffer meewerkt, verkrijgen de oplichters toegang tot de computer van het slachtoffer en maken op verschillende wijzen geld buit (Op basis van Veiliginternetten.nl, *z.d.*).

Wat hebben jullie onderzocht?

De risicoperceptie en het preventieve gedrag van ouderen (65+) in de regio's Twente en de Achterhoek met betrekking tot helpdeskfraude en welke interventies ingezet kunnen worden om de risicoperceptie en preventieve gedrag onder deze doelgroep te bevorderen.

Waarom hebben jullie dit onderzocht?

Bij helpdeskfraude vindt telefonisch contact plaats met iemand die zich voordoet als medewerker van een bedrijf. Bij deze vorm van cybercrime worden de slachtoffers ervan overtuigd dat er problemen zijn ontdekt op hun computer en dat deze (niet bestaande) problemen alleen door de persoon aan de andere kant van de lijn tegen betaling kunnen worden opgelost. Helpdeskfraude is een probleem voor ouderen, omdat zij doorgaans weinig technische kennis over computers hebben en daarom eenvoudig(er) zijn op te lichten. Dit kan voor hen veel financiële en emotionele schade opleveren. Bij de Fraudehelpdesk is bekend dat er van deze vorm van cybercriminaliteit de meeste meldingen gedaan worden door 55+'ers.

Hoe hebben jullie dit onderzocht?

Om de aard en omvang van helpdeskfraude in beeld te brengen hebben wij een literatuurstudie uitgevoerd. Daarbij gebruikten wij verschillende bronnen, bijvoorbeeld internetbronnen geschreven door deskundigen en nieuwsartikelen die (historische) gebeurtenissen toelichten en algemene cijfers verschaffen. Om de risicoperceptie en het preventieve gedrag van de ouderen in kaart te brengen is kwalitatief onderzoek uitgevoerd. Wij hebben in totaal elf interviews gehouden met 65+'ers die in de Achterhoek of in Twente wonen.

Wat waren jullie belangrijkste bevindingen?

Uit de interviews bleek dat de risicoperceptie van deze doelgroep ten aanzien van helpdeskfraude vrij hoog is. Zij zijn zich niet bewust van de term 'helpdeskfraude', maar weten na onze uitleg wel wat het is. Verder bestaat er veel wantrouwen onder de doelgroep ten opzichte van onverwachte telefoontjes van onbekende bellers. De kennis over de gevaren en risico's van de doelgroep komt vooral voort uit aandacht voor deze cybercrime van televisieprogramma's (n=7); de invloed van de omgeving (n=6) en verhalen over deze vorm van fraude in de krant (n=1).

Verder troffen wij ook sporen van een *optimistic bias* ten aanzien van helpdeskfraude onder de doelgroep. Men ziet voor zichzelf een heel klein risico maar zegt gelijktijdig *"Het overkomt de ander wel, maar mij niet".* Verder blijkt dat het grootste deel al preventief gedrag vertoont om schade door helpdeskfraude te voorkomen. Aan de andere kant blijkt dat iets meer dan de helft van onze respondenten geen investering wil doen in de vorm van geld, tijd of moeite om verdere maatregelen te nemen. Het grootste deel van de respondenten zou naar eigen zeggen wel melding doen bij een instantie op het moment dat ze slachtoffer zijn geworden. Daarbij verwachten zij het meeste van hun bank.

Hoe kan slachtofferschap van helpdeskfraude onder ouderen volgens jullie worden tegengegaan?

De risicoperceptie en het preventieve gedrag ten aanzien van helpdeskfraude onder ouderen kan volgens ons aanzienlijk worden verhoogd door:

I. Een simulatie waarin getest wordt of mensen slachtoffer worden van helpdeskfraude ('Helpdeskfraude, trapt u erin?');
II. Een poster en folder met tekstuele ondersteuning ten aanzien van helpdeskfraude ('Helpdeskfraude: Blijf alert!'). Er worden hierbij tips gegeven over "Hoe herken ik helpdeskfraude? , "Hoe bescherm ik mijzelf?", "Ik ben gebeld, wat nu?", "Help! Ik heb mijn bankgegevens doorgegeven, wat nu?";
III. Het gebruik van *story telling:* het verhaal van een ouder slachtoffer om hiermee het risico van helpdeskfraude meer te laten leven voor de potentiële slachtoffers. Doordat er gebruik gemaakt wordt van ervaringsverhalen wordt volgens ons zowel de risicoperceptie als de affectieve respons versterkt.


Mobile Banking
Login
Password
Login

Tikkiefraude

Laurens Flierman (Security Management)
Justin Bos (Integrale Veiligheidskunde)
Pip Schuiling (HBO Rechten)

Tikkiefraude Oplichting via een realistische kopie van de betaaldienst Tikkie, waardoor bank-inloggegevens van slachtoffers buit worden gemaakt of een groter bedrag wordt afgeschreven dan is overeengekomen via het sturen van een frauduleuze betaallink aan slachtoffers (op basis van Slachtofferhulp.nl, *z.d.*).

Wat hebben jullie onderzocht?

De risicoperceptie en het preventieve gedrag van marktplaatsgebruikers tussen de 35 en 45 jaar oud, met betrekking tot betalingsfraude door middel van betaalverzoeken via de betaalapp Tikkie.

Waarom hebben jullie dit onderzocht?

Tikkiefraude kan onder slachtoffers tot financiële en psychische schade leiden. De dader doet zich via Marktplaats voor als koper van een product. Daarbij doet de dader het voorkomen dat hij eerder zelf is opgelicht en vraagt zijn slachtoffer om via Tikkie een verwaarloosbaar klein bedrag over te maken te kunnen controleren of de betaling goed doorkomt. Wat het slachtoffer niet weet, is dat het verzoek met het verwaarloosbaar kleine bedrag leidt naar een nep Tikkie-omgeving. De omgeving waar de verkoper via een link naar toe gestuurd wordt, is een nagemaakte betaalomgeving die bijna identiek is aan de betaalomgeving van de Tikkie-app. Wanneer de verkoper argeloos het kleine bedrag overmaakt, gebruikt de crimineel de betaalgegevens direct om toegang te krijgen tot het online bankieren van de verkoper en boekt snel grote bedragen over.

Hoe hebben jullie dit onderzocht?

Om het beeld van feiten en informatie omtrent Tikkiefraude te schetsen hebben wij literatuuronderzoek gedaan. Om de risicoperceptie en het preventieve gedrag te onderzoeken hebben wij kwalitatief onderzoek gedaan. Wij hebben interviews gehouden met elf Marktplaatsgebruikers tussen de 35 en 45 jaar en een expert op het gebied van fraude.

Wat waren jullie belangrijkste bevindingen?

De risicoperceptie onder onze respondenten bleek laag. Meer dan de helft van de respondenten wist niet af van het bestaan van Tikkiefraude. Tijdens de gehouden interviews is gebleken dat de ondervraagden zichzelf niet zien als de primaire slachtoffergroep van Tikkiefraude. Elke respondent gaf aan de kans om zelf het slachtoffer van Tikkiefraude te worden heel laag in te schatten, want dat overkomt vooral anderen. Maar de respondenten konden gelijktijdig – behalve het vermijden van de Tikkiebetalingen - geen maatregelen benoemen die zij al tegen dit risico hadden genomen of in de toekomst zouden kunnen nemen. Daarmee is er volgens ons sprake van een *optimistic bias*.

Hoe kan slachtofferschap van Tikkiefraude onder 35 tot 45 jarigen volgens jullie worden tegengegaan?

De risicoperceptie en het preventieve gedrag kan volgens ons aanzienlijk worden verhoogd als de verschillende stakeholders de onderstaande acties uitvoeren:

I. Banken moeten een dagelijks limiet op betaalapps instellen. Zo wordt de schade voor het slachtoffer beperkt en de winst voor de daders kleiner.
II. Gebruikers van betaal apps moeten 2 factor authenticatie aanzetten. Wanneer zij hun inloggegevens invullen op een namaak website ontvangen zij geen bericht op hun mobiele telefoon, waardoor eventuele oplichtingspogingen worden ontdekt. Ook kunnen daders via de 2 factor authenticatie niet langer alleen met de inloggegevens overboeken.

III. Marktplaatsgebruikers kunnen veilig betalen via de ‘gelijk oversteken’ dienst van het platform. Zo zijn er geen betaalverzoeken via andere websites of apps nodig.
IV. Marktplaats zou geautomatiseerd een pop-up-melding kunnen geven wanneer je in gesprek gaat met een mogelijke koper. Bij deze melding worden de tips om veilig te handelen weer gegeven. Dit zorgt ervoor dat je als gebruiker op het juiste moment, de juiste informatie krijgt om jezelf tegen oplichting te weren.
V. Marktplaats moet frauduleuze gebruikers actief opsporen en blokkeren. Door middel van verschillende en deels geautomatiseerde controles kunnen zij voorkomen dat deze oplichters opnieuw accounts aanmaken op Marktplaats.
VI. Het moet op Marktplaats makkelijker worden gemaakt om advertenties en gebruikers als verdacht te markeren of te rapporteren.
VII. Als gebruikers de betaalapp Tikkie downloaden zou een goede interventie zijn dat zij voor gebruik van de app verplicht op het risico van fraude worden gewezen.


WE´RE
HIRING

Vacaturefraude

Ramona Linschoten (Security Management)
Melanie Prins (Security Management)
Jennifer Helder (HBO Rechten)

Vacaturefraude Bij vacaturefraude worden slachtoffers met nep vacatures verleid tot het doen van betalingen of het prijsgeven van persoonlijke gegevens waarmee vervolgens identiteitsfraude wordt gepleegd (op basis van Jobsonline.nl, *z.d.*).

Wat hebben jullie onderzocht?

Wij hebben de risicoperceptie en het preventie gedrag van werkzoekende Nederlanders tussen de 18 en 27 jaar ten aanzien van vacaturefraude onderzocht. Ook hebben we onderzocht hoe de risicoperceptie en het preventieve gedrag onder deze doelgroep kan worden verbeterd.

Waarom hebben jullie dit onderzocht?

Vacaturefraude is een vorm van identiteitsfraude waarbij criminelen persoonsgegevens verkrijgen door middel van het online plaatsen van onechte vacatures. Wanneer werkzoekenden hierop reageren door het achterlaten van gegevens kunnen criminelen deze gebruiken voor criminele doeleinden, zoals het openen van een bankrekening op naam van het slachtoffer. Dit kan tot financiële en emotionele schade bij het slachtoffer leiden.

Hoe hebben jullie dit onderzocht?

Om inzicht te krijgen in de risicoperceptie en het preventieve gedrag hebben wij literatuuronderzoek gedaan en interviews gehouden met twaalf mensen uit de doelgroep. Om inzicht te krijgen in mogelijke interventies hebben wij nogmaals literatuuronderzoek uitgevoerd. Voor beide literatuurstudies hebben wij gebruik gemaakt van wetenschappelijke literatuur, jurisprudentie, naslagwerk en internetbronnen.

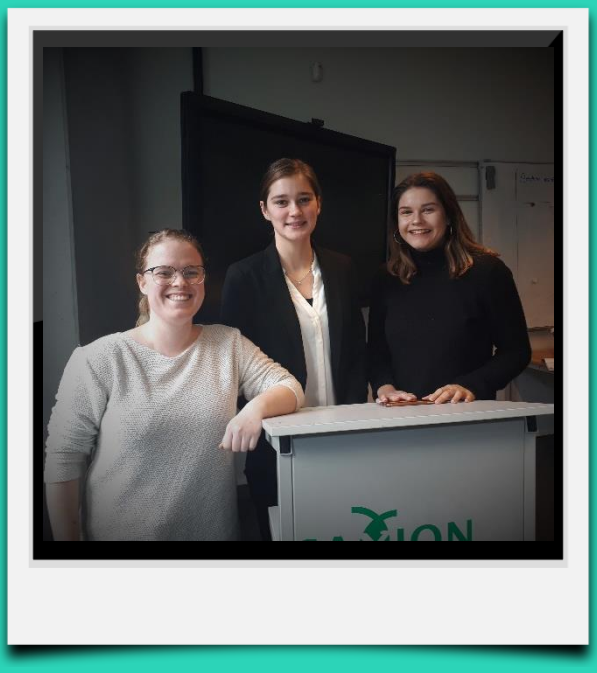
Wat waren jullie belangrijkste bevindingen?

Het meest opvallende was dat een aantal respondenten nog niet van vacaturefraude had gehoord, of niet wisten wat de gevolgen zouden kunnen zijn. Verder gaven respondenten aan niet te weten hoe je vacaturefraude zou kunnen herkennen. Al met al was deze vorm van identiteitsfraude dus nog zeer onbekend onder onze respondenten. Vreemd genoeg gaven de respondenten gelijktijdig aan dat zij hun risicoperceptie hoog inschatten, maar gevolgen of kenmerken van een nep-vacature konden ze niet benoemen.

Het blijkt dat er nog weinig interventies bestaan om slachtofferschap van vacaturefraude te voorkomen. De meeste vacaturesites hebben wel een pagina waarop staat waar je op moet letten als je online gaat solliciteren, maar deze pagina staat meestal ergens achteraf en daar moet flink naar worden gezocht. Toch kunnen de meeste interventies die betrekking hebben op identiteitsfraude ook voor vacaturefraude worden toegepast, zoals de KopieID app voor het veilig versturen van het ID of https://checkjelinkje.nl/ voor de controle van het linkje.

Hoe kan slachtofferschap van vacaturefraude onder mannen en vrouwen tussen de 18 en 27 jaar wonend in Nederland volgens jullie worden tegengegaan?

De risicoperceptie kan volgens ons aanzienlijk worden verhoogd door een AR-applicatie. AR (*Augmented Reality*) is het uitbreiden van de echte wereld met virtuele elementen. Het voordeel van AR is dat het toegankelijk is voor iedereen die een smartphone met camera heeft. Op fysieke plekken waar de doelgroep vaak komt, moet een aantrekkelijke advertentie komen. Deze advertentie bevat een QR-code en wanneer deze gescand wordt met een telefoon opent de AR-applicatie op de telefoon. De gebruiker van de applicatie maakt daarmee op realistische wijze kennis met een crimineel die uit is op persoonsgegevens. De gebruiker zit bij wijze van spreken samen met de crimineel op de bank. De crimineel krijgt vervolgens bankgegevens en een BSN-nummer te pakken en sluit hiermee abonnementen af. Op deze manier krijgt de gebruiker te zien wat een crimineel kan met welke persoonsgegevens.




Message

Smishing

Emma van Berkum (Integrale Veiligheidskunde)
Leon van den Bedem (Security Management)
Manon Frankenhuizen (HBO Rechten)
Han Bleumer (Security Management)

Smishing Dit is de sms-variant van *phishing*. Het verzonden sms-bericht bevat een link die het slachtoffer op zijn of haar smartphone naar een website stuurt die kwaadaardige software installeert of omleidt naar een frauduleuze website die lijkt op de digitale bankomgeving om de bankgegevens van het slachtoffer buit te maken of het slachtoffer op andere wijze geld afhandig te maken. (Op basis van Dfbonline.nl, *z.d.*).

Wat hebben jullie onderzocht?

De risicoperceptie en het preventieve gedrag van Oost-Nederlandse 25 tot 65-jarigen bij de cybercrime “smishing” waarbij de aanvaller zich via een sms voordoet als particuliere bank en welke interventies de risicoperceptie te vergroten en het preventieve gedrag kunnen stiumuleren.

Waarom hebben jullie dit onderzocht?

De Nederlandse samenleving is afhankelijk van digitale systemen. Mobiele telefoons worden gebruikt als communicatiemiddel, maar tegenwoordig ook om bankzaken mee te regelen. Cybercriminelen sturen steeds vaker nepberichten met de intentie om betaalgegevens te ontfutselen (phishing) door middel van sms'jes (smishing) die afkomstig lijken te zijn van banken. De maatschappelijke schade van smishing zal waarschijnlijk in de miljoenen euro’s lopen. Ook ziet de politie een sterke stijging in phishing via dergelijke sms-berichten.

Hoe hebben jullie dit onderzocht?

Om kennis op te doen over smishing hebben wij allereerst literatuuronderzoek gedaan. Om de risicoperceptie en het preventieve gedrag te onderzoeken hebben wij voor kwalitatief onderzoek gekozen. Wij hebben wij met twaalf potentiële slachtoffers tussen de 25 en de 65 jaar oud die woonachtig zijn in Gelderland of Overijssel een semigestructureerd interview gehouden. Ook hebben we de security experts van twee banken geïnterviewd.

Wat waren jullie belangrijkste bevindingen?

Slechts een paar respondenten wisten ons direct te vertellen wat smishing is. Na een toelichting bleek ongeveer de helft van de respondenten ooit een vals sms-bericht te hebben ontvangen. Onze respondenten waren er unaniem van overtuigd dat hun bank hen eigenlijk nooit sms-berichten stuurt. Wanneer een respondent toch een sms-bericht ontvangt dat vals lijkt te zijn wordt het sms-bericht verwijderd. Vier respondenten kijken bij het ontvangen van de berichten naar eigen zeggen naar de afzender en of de spelling in het bericht klopt. Ook werd aangegeven dat gekeken wordt of er inloggegevens moeten worden ingevuld. Ten slotte gaf een enkele respondent aan te kijken naar de algemene autoriteit die het bericht uitstraalt. Toch gaven bijna alle respondenten aan dat er een kans bestaat dat ze slachtoffer kunnen worden van dit misdrijf.

Niet alle respondenten weten even goed wat ze moeten doen als ze een smishing bericht krijgen en hoe ze verder moeten handelen wanneer ze in een smishing bericht zijn getrapt. Hierbij geven enkele respondenten aan dat ze de bank zullen bellen bij het krijgen van een smishing bericht en wanneer zij slachtoffer zijn geworden. De respondenten gaven tevens aan dat ze meteen hun rekeningen en pinpassen zouden blokkeren. Tijdens het bespreken van de gevolgen van het openen en invullen van een smishing bericht kwam naar voren dat veel respondenten weten dat er grote gevolgen kunnen zijn. Vooral de financiële schade wordt als groot ingeschat. Een enkele respondent noemde de tijd en moeite die gepaard gaat met het regelen van het blokkeren van de rekening en het oplossen van het slachtofferschap.

Ongeveer de helft van de geïnterviewde respondenten vindt dat er voldoende aandacht wordt besteed aan smishing. Een kleine meerderheid van de respondenten heeft hierover informatie gehad via de televisie, bijvoorbeeld in het nieuws en via voorlichtingsspotjes. Dit heeft de risicoperceptie van de respondenten naar eigen zeggen verhoogd.

Hoe kan slachtofferschap van smishing binnen de doelgroep volgens jullie worden tegengegaan?

De risicoperceptie en het preventieve gedrag kan volgens ons aanzienlijk worden verhoogd door onderstaande acties uit te voeren:

I. De consumenten moeten risicobewust gemaakt worden van smishing op social media door middel van advertenties.
II. Wij adviseren de banken om naar één communicatiekanaal over te gaan, de persoonlijke omgeving van de klant op de website of de app van de desbetreffende bank.

Geraadpleegde literatuur

CBS (2018). *Cybersecuritymonitor 2018. Een verkenning van dreigingen, incidenten en maatregelen.* Den Haag: CBS.

De Jong, J. (2018). *Het mysterie van de verdwenen criminaliteit*. Den Haag: CBS.

Dfbonline.nl (z.d.). *Sexting en shame sexting* . Via: https://www.schoolenveiligheid.nl/mbo/kennisbank/sexting-en-shame-sexting/

Farrell, G, Tseloni, A., Mailley, J. & Tilley, N. (2011). The crime drop and the security hypothesis. *Journal of Research in Crime and Delinquency*, 48(2), 147-175.

Farrell, G., Tilley, N. & Tseloni, A. (2014). Why the crime drop? *Crime and justice*, 43(1), 421-490.

Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior*, 35(1), 20-40.

Holt, T.J. Bossler, A.M. & Seigfried-Spellar, K.C. (2018). *Cybercrime and Digital Forensics: An Introduction*. New York: Routledge.

Jobsonline.nl (z.d.). *Vacaturefraude uitleg*. Via: https://www.jobsonline.nl/nieuws/vacaturefraude-uitleg/

Kleve, P., De Mulder, R. & Van Noortwijk, K. (2011). The definition of ICT Crime. *Computer Law & Security Review*, 27(2), 162-167.

Leukfeldt, E. R., & Kleemans, E. E. (2019). Cybercrime, money mules and situational crime prevention. *Criminal Networks and Law Enforcement: Global Perspectives On Illegal Enterprise*, 13.

Leukfeldt, E.R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Den Haag: Eleven International Publishers.

Slachtofferhulp.nl (z.d.). *Tikkiefraude*. Via: https://www.slachtofferhulp.nl/gebeurtenissen/fraude/tikkiefraude/

Spithoven, R. (2020). *Verbonden risico's. Maatschappelijke veiligheid in de black box society.* Den Haag: Boom Criminologie.

Van Dijk, J.J.M., Tseloni, A. & Farrell, G. (Eds.). (2012). *The international crime drop: New directions in research*. Londen: Palgrave MacMillan.

Veiliginternetten.nl (z.d.). *Wat is helpdeskfraude?* Via: https://veiliginternetten.nl/themes/situatie/wat-helpdeskfraude/

Gebruikte afbeeldingen (vrij te gebruiken incl. aanpassingen)

Afbeelding omslag via:
https://www.needpix.com/photo/871176/hacking-cyber-crime-security-hacker-internet-computer-technology-virus-protection

Polaroidframe via:
https://freesvg.org/smerrell-polaroid

Afbeelding blocknote (p. 2) via:
https://www.cleanpng.com/png-desktop-wallpaper-notebook-notepad-mobile-phones-p-900612/preview.html

Afbeelding trap (p. 3) via:
https://commons.wikimedia.org/wiki/File:Steps.svg

Afbeelding cybercrimineel (p. 5) via:
https://www.piqsels.com/en/search?q=firewall

Afbeelding sextortion (p.5 & 12) via:
https://www.schriever.af.mil/News/Article-Display/Article/1083485/sextortion-scams-on-the-rise/

Afbeelding money mules (p. 5 & 16) via:
https://www.flickr.com/photos/149561324@N03/45773469574

Afbeelding ransomware (p. 5 & 20) via:
https://pixabay.com/nl/photos/ransomware-cybercriminaliteit-2320941/

Afbeelding helpdeskfraude (P. 5 & 24) via:
https://upload.wikimedia.org/wikipedia/commons/8/83/Call_center_agent.jpg

Afbeelding tikkiefraude (P. 5 & 28) via:
https://www.pxfuel.com/en/free-photo-xdzua

Afbeelding vacaturefraude (P. 5 & 32) via:
https://pixabay.com/nl/photos/baan-vacature-werkplek-baan-zoeken-2860035/

Afbeelding smishing (p. 5 & 36) via:
https://flickr.com/photos/160866001@N07/48049158838/

Studenten vanuit verschillende opleidingen begeleiden tijdens een praktijkopdracht. Samenwerken in multidisciplinaire groepen. Ik ben erachter gekomen dat dat absoluut meerwaarde heeft. Het was mooi om te zien hoe studenten vanuit hun eigen discipline, elkaar versterken en zo samen tot mooie resultaten kwamen. De prettige samenwerking met het lectoraat Maatschappelijke Veiligheid maakte alles tot een prachtig geheel. Dit smaakt naar meer!

Mr. Ben den Tuinder – Begeleidend docent-onderzoeker uit het team Security Management

Het onderzoek binnen de minor met als thema Cyberweerbaarheid zorgde voor een nieuwe uitdaging op het gebied van multidisciplinair samenwerken tussen studenten en docenten afkomstig uit verschillende opleidingen. Een sprong in het diepe, soms even terug naar de tekentafel, de schouders er onder en een focus houden. Ik ben als begeleidend docent trots op de onderzoeksresultaten die de studenten hebben gepresenteerd en de mooie samenwerking met het lectoraat Maatschappelijke Veiligheid, dat zeker in de toekomst een vervolg zal krijgen!

Mr. Christine Vording – Begeleidend docent-onderzoeker uit het team HBO Rechten

Het was een enorm leergierige groep studenten die allemaal hun tanden hebben gezet in een specifieke vorm van cybercrime. Het feit dat ze veelal afkomstig waren van verschillende opleidingen maakte dat ze ook allemaal hun eigen rol hadden in het project evenals hun eigen kijk op het onderwerp. De samenwerking tussen Ben, Christine en mijzelf als begeleiders enerzijds en Remco en Ynze vanuit het lectoraat anderzijds was een feestje! Kortom; op naar de tweede lichting studenten in 2020!

Mr. Mark Dorenbusch – Begeleidend docent-onderzoeker uit het team Bestuurskunde

Hogeschool Saxion
Lectoraat Maatschappelijke Veiligheid
2020

SAXION
UNIVERSITY OF APPLIED SCIENCES