Veiligheid & Mobiel bankieren

Door Tomas Rijnbeek - Specialisatie User Experience Design

Docent:	Thijs Waardenburg
Studentnummer:	1680150
Cursus:	Seminar
Cursuscode:	JDE-SEMUX.3V-13_2017
Datum:	12-01-2018
Woorden:	3747

Voorwoord

Voor u ligt het onderzoek “Veiligheid & user experience bij mobiel bankieren.” Dit onderzoek is gemaakt in het kader van mijn specialisatie user experience design als onderdeel van het vak ‘Seminar’ dat wordt aangeboden tijdens mijn opleiding Communicatie en Multimedia Design aan de Hogeschool Utrecht.

Ik wil graag mijn docent, Thijs Waardenburg, bedanken voor het helpen opzetten voor het onderzoek. Daarnaast wil ik graag UX designers van de ING Cornelis Moens en Arnoud Snippert bedanken voor de verhelderende interviews die nieuwe inzichten hebben kunnen opdoen voor het onderzoek.

Ik wens u veel leesplezier.

Tomas Rijnbeek
12-01-2018

Inhoudsopgave

1.1 Inleiding.

Aan het begin van dit onderzoek was het mijn streven om een stage te doen bij een bank. Ik ben daarom blij om te vermelden dat dit mij gelukt is en ik vanaf 5 februari 2018 werkzaam ben als stagiair Interaction Designer voor de ING.

In eerste instantie had ik al veel bewondering voor de mobiel bankieren app van de ING. Ik ervaar de user experience van deze app namelijk als zeer goed omdat hij moeizame en gevoelige processen heel erg versimpelt. Daarom wilde ik hier wel een kijkje achter de schermen door middel van een stage. Een bank is een grote organisatie en daar is de mogelijkheid om omringt te zijn met veel specialisten op het gebied van user experience.

Nederland loopt erg voor met internet/mobiel bankieren. Het digitaliseren van banken is een proces wat op heel veel plekken op de wereld aan het gebeuren is. Om deze reden denk ik dat op het gebied van user Experience hier veel te halen en te leren valt. Om mij vast goed te profileren en voor te bereiden op de stage widel ik onderzoek doen naar privacy en veiligheid en hoe die invloed hebben op mobiel bankieren. Hierover heb ik ook kort gesproken met Maartje van Hardeveld, lead UX designer bij de Rabobank, die mij vertelde dat privacy en veiligheid echt een knelpunt zijn voor de user experience. Hierop volgend is er bij mij voor dit vak een onderzoek gestart.

1.2 Methoden

Voor dit onderzoek heb ik verschillende onderzoeksmethode toegepast om tot een conclusie te komen.

Interviews:
Bij de interviews heb ik allemaal geprobeerd door te vragen op gedachten die geïnterviewde had om zo tot de kern te komen van het vraagstuk. Ik heb vragen gesteld die niet direct in betrokking stonden tot veiligheid omdat ik mensen niet wilde beïnvloeden over hun gedachten over de applicatie. Op deze manier heb ik geprobeerd een zo natuurlijke mogelijke respons te krijgen.

professionals
Met professionals van de ING (Cornelis Moens & Arnoud Snippert) heb ik gesproken over wat voor beveiligingen er allemaal worden toegepast binnen de mobiele applicatie en hoe deze invloed hebben op de user experience. Deze mensen heb ik bereikt door middel van een doorverwijzing van Bernard Weerdmeester voor een stagegesprek bij de ING.

Gebruikers
Met gebruikers heb ik kunnen sparren over hoe ze de applicatie gebruiken, wat ze denken over de beveiliging en welke gevoelens deze oproepen.

Deskresearch
Cijfers en statistieken die vanuit de banken zijn gekomen zijn gebruikt in het onderzoek, daarnaast zijn bronnen gebruikt van de webpagina's en onderzoeken van de banken om achter algemene informatie en werkwijze te komen.

Analyse
Door middel van analyse van de communicatie van de banken over de applicatie kan worden gekeken hoe de bedrijven de gebruiker veilig laat voelen. Daarnaast is er gebruik gemaakt van analyse om te kijken wat voor soorten beveiligingen er worden toegepast.

2.1 Hoofdvraag

“Op welke manier heeft veiligheid invloed op de user experience bij mobiel bankieren?”

Om tot een valide conclusie te komen op de hoofdvraag zijn de volgende deelvragen opgesteld:

2.2 Deelvragen

1. Wat is mobiel bankieren?

2. Welke vormen van beveiliging gebruiken banken op een mobiel bankieren app?

3. Hoe zorgen banken dat klanten zich veilig voelen tijdens het mobiel bankieren?

4. Welke gevoelens roept beveiliging op bij de gebruiker bij mobiel bankieren?

5. Heeft de beveiliging invloed op de user flow (het uitvoeren van taken)?

2.3 Hypothese

Veiligheid heeft invloed op user experience in de vorm van een beveiliging zoals verificatie. Hierdoor kan de gebruiker niet direct een actie volbrengen en dit kan als hinderlijk worden ervaren. De veiligheid is in vele gevallen een negatieve invloed op de user experience.

3. Wat is mobiel bankieren?

Nederland loopt erg vooruit met de manier waarop wij bankieren Zo blijkt dat 83 procent van de Nederlanders gebruik maken van internet bankieren. (Emerce, 2017)[1]. Onder internet bankieren verstaan we bankzaken doen via het internet. Hierbij kan er worden gedacht aan dingen zoals geld overmaken en saldo checken. Deze bankzaken door middel van internet kan worden gedaan op een computer, laptop, smartphone of tablet. Wanneer de bankzaken worden gehanteerd vanuit een mobiel apparaat, zoals de smartphone, spreken we over mobiel bankieren.

Wanneer er binnen dit onderzoek wordt gesproken over mobiel bankieren, dan wordt er gerefereerd naar bankzaken doen door middel van een door de bank ontworpen mobiele applicatie.

1) Redactie Emerce. (2017, 22 februari). ‘Nederlanders nemen het voortouw bij het internetbankieren’. Geraadpleegd van https://www.emerce.nl/nieuws/nederlanders-nemen-voortouw-internetbankieren

4. Welke vormen van beveiliging gebruiken banken op een mobiel bankieren app?

ING beweert dat 55 procent van alle Nederlanders een mobiele applicatie gebruikt om bankzaken mee te doen. (ING - feiten en cijfers, 2016)[2]. Er zijn dus veel mensen die een mobiel apparaat mee hebben en daarmee ook hun bankzaken in hun broekzak hebben zitten. Daar moeten veel verschillende soorten beveiligingen voor zijn om al deze informatie veilig te behouden. Om te weten hoe al deze beveiligingen invloed hebben op de user experience moet eerst worden vast gesteld welke beveiligingen er allemaal zijn.

De beveiligingen zijn naar eigen inzicht onderverdeeld in de volgende categorieën en zo gepresenteerd tijdens het seminar om het overzicht te bewaren.

Toegang

Beveiligingen met betrekking tot het toegang krijgen tot alledaagse gebruik van de applicatie voor het handelen van je bankzaken.

Cijfercode
De persoonlijke cijfercode is een door de gebruiker gemaakte code waar om gevraagd wordt bij het inloggen van de applicatie. Dit is de primaire manier van inloggen op de applicatie. Echter kan hij ook als secundaire mogelijkheid van inloggen zijn bij het gebruik van een vingerafdruk, spraak- of gezichtsherkenning. Deze cijfercode dient ook als beveiligingen bij het valideren bij een transactie.

Vingerafdruk, gezichtsherkenning & stemherkenning
Deze drie functionaliteiten worden mogelijk gemaakt door de telefoon zelf waar de applicatie gebruik van kan maken. Door middel van een scan van het topje van je vinger, gezichts- of stem analyse kan toegang tot de app worden verleend of overschriften worden bevestigd.

Beperkte inlogpogingen
Bij het mobiel bankieren kan er maar een beperkt aantal keer een poging tot inloggen worden gedaan. Dit is een stuk preventie vanuit de bank om ervoor te zorgen dat iemand niet ongewenst bij een rekening kan komen. Wanneer de er meer dan bijvoorbeeld drie inlogpogingen zijn gedaan wordt de applicatie geblokkeerd waarna de bank gecontacteerd moet worden.

automatische uitlog
Soms wordt een applicatie verlaten maar niet afgesloten. Wanneer er vanuit een applicatie wordt genavigeerd naar een vorig/thuis scherm zorgt de telefoon normaliter dat de applicatie in stand wordt gehouden dat de gebruiker bij heropening van de app direct verder kan. Echter zitten bij mobiel bankieren een functionaliteit ingebouwd dat de gebruiker wordt uitgelogd na een paar minuten van het verlaten van de applicatie. Zo wordt er voorkomen dat een ongewenst persoon verder kan waar de gebruiker hun bankzaken had achtergelaten.

Encryptie
Niet alle beveiligingen die met toegang te maken hebben zijn zichtbaar. Zo zegt Arnoud Snippert, UX Designer bij ING, dat er voor de applicatie van de ING een speciaal geschreven encryptie is. Dit houdt in dat er een systeem is dat de informatie op, van en naar de applicatie versleuteld wordt zodat deze niet van buitenaf te achterhalen is en mensen niet op de applicatie kunnen inbreken.

Verificatie

Verificatie heeft betrekking met het valideren van gegevens of identiteit zodat de kans op oplichting of ongewenste transacties wordt geminimaliseerd.

Bevestigingsscherm
Wanneer er door de gebruiker een overschrift wordt gedaan wordt er nog een bevestiging laten zien met alle ingevulde informatie zodat de gebruiker zeker weet dat de juiste informatie is ingevuld. Deze beveiliging is preventie voor foutief noteren van informatie die gevolg kan hebben voor het overschrijven van een verkeerd bedrag of naar een onjuist persoon.

Twee-stap verificatie
Een twee-stap verificatie is bedoeld om identiteit te valideren van een persoon. Een extra code, die eventueel binnen komt op ander apparaat, die in bezit is van de eigenaar van de rekening zorgt ervoor dat het overschrijven van geld niet met een enkele beveiliging gedaan kan worden. Door de extra stap die genomen wordt die alleen kan worden uitgevoerd met het juiste middel die in het bezit is van de eigenaar van de rekening wordt de identiteit gevalideerd. De twee-stap verificatie is in het kader van mobiel bankieren op meerdere manieren mogelijk.

QR Code
Bij internetbankieren verschijnt er op het computerscherm bij een betaling een QR-code op het scherm die met de applicatie gescand kan worden. De applicatie zorgt voor de verificatie van identiteit omdat alleen de eigenaar van de rekening binnen de applicatie kankomen.

Identifier / random reader / card reader
Al de bovengenoemde items zijn apparaatjes waarmee identiteit bevestigd kan worden doordat de gebruiker deze in bezit heeft. Op verschillende manieren kan een betaling hiermee worden bevestigd. De identifier van ABN geeft een unieke code, de random reader van Rabobank genegeerd een code die gescand kan worden en de card reader van bijvoorbeeld knab moet je bankpas in worden gevoerd om je pincode in te voeren en daarmee je identiteit te bevestigen.

2)ING Group. (z.j.). Feiten en Cijfers. Geraadpleegd van https://www.ing.nl/nieuws/feiten_en_cijfers/index.html

Bevestigingscode
Een bevestigingscode kan ontvangen worden per mail of sms door de gebruiker om de applicatie te activeren. Zo wordt de bank zeker dat de applicatie wordt geactiveerd door de juiste persoon doordat de code wordt verzonden naar een persoonlijk middel.

Schadebeperking

Externe controle
In het interview met Cornelis Moens, lead UX designer bij ING, dat er achter de schermen van de applicatie een geheel cyberthreat team is dat alle gevaren van hacken en opmerkelijk transacties in de gaten worden gehouden. Er worden op verschillende vlakken controle gehouden:

Locatie
Wanneer er vanuit twee verschillende locaties transacties worden gemaakt en dit als fysiek onmogelijk wordt beschouwd voor de gebruiker om zich in korte tijd op twee verschillende punten te begeven komt er een melding waarna er wordt gecontroleerd of de transactie wel van de gebruiker zelf kwam.

Grote bedragen
Bij een ongebruikelijk groot bedrag wordt de applicatie in de gaten gehouden om te kijken of het geld wel van of naar een legitieme bestemming gaat.

Onbekende personen
Ook in relatie tot grote bedragen naar onbekende personen wordt een account in de gaten gehouden.

Wanneer er op 1 of meerdere van deze vlakken zich exorbitante gevallen voordoen kan de applicatie extern worden geblokkeerd vanuit de ING en wordt de gebruiker gecontacteerd of de transacties wel gewenst waren en of alles wel legitiem gebeurd.

Daglimieten
Via de applicatie kan de gebruiker een geldbedrag als limiet instellen die niet kan worden overschreden met de applicatie of bankpas.

Geld terughalen
Wanneer er een afschrift van je rekening is gedaan kan deze (in sommige gevallen) worden teruggehaald binnen de applicatie.

Screenshot beveiliging
Op sommige applicaties kunnen er geen screenshots worden gemaakt. Dit zorgt ervoor dat er geen persoonlijke of gevoelige informatie naar buiten kan worden gestuurd.

Externe blokkering
Mocht er zich een situatie voordoen zoals omschreven onder “controle” kan de applicatie extern worden geblokkeerd. Daarnaast kan de gebruiker vanuit de website of klantenservice van de bank de applicatie laten blokkeren wanneer de persoon in kwestie niet meer in bezit is van zijn of haar mobiele apparaat.

Informatie uitwisseling
De Nederlandse Vereniging van Banken zorgt ervoor dat de financiële instellingen met elkaar informatie uitwisselen over criminelen en de werkwijze van hen. Zo zijn de banken beter voorbereid op eventuele aanvallen op zo ook de applicaties.

De filosofie van ING betreffende beveiliging

Cornelis Moens, lead UX designer bij ING, heeft verteld dat de ING met drie verschillende aspecten bezig is als het gaat om veiligheid. Deze zijn als volgt:

1. Je hebt de app nodig

Je moet op de applicatie geregistreerd zijn waarvoor je identificatie bevestigd moet zijn

2. Je hebt kennis nodig

Iets van persoonlijke kennis wat alleen in jouw bezit is. Dit is vaak iets persoonlijks zoals een code maar kan ook bijvoorbeeld een fingerprint zijn.

3. Je hebt de bank nodig

Dat de bank nodig is klinkt vanzelfsprekend, maar hier wordt mee bedoeld dat de gebruiker zeker moet zijn dat de ING wel daadwerkelijk degene is die de app aanbied. Anders kan de klant van de bank misleid worden met een verkeerde app. De bank is er dus ook mee bezig om identiteit te bevestigen dat de gebruiker zich veilig voelt omdat hij of zij zeker weet dat er met de juiste instantie wordt gehandeld.

Het gevoel van veiligheid haakt in op de volgende deelvraag:

5.Hoe zorgen banken dat klanten zich veilig voelen tijdens het mobiel bankieren?

Trust en Security model

Er zijn verschillende manieren waarop de bank de klant zich veilig laat voelen. Bij de onboarding van de applicatie moet de gebruiker zich veilig voelen en tijdens het gebruik ervan ook. Rabobank heeft in samenwerking met de Universiteit Twente onderzoek gedaan naar consument acceptatie betreffende betalingen op de mobiele telefoon. (A. de Roos, 2011)[1] Rabobank heeft voor het gebruik van de applicatie gekeken naar een security & trust model dat opgesteld is door Kim, C., W. Tao, et al. (2010) [2]. Hierin staan vier verschillende punten die zorgen voor (gevoel) van veiligheid en vertrouwen:

Toelichting schema

1. Technical protection
2. Security statements
3. Perceived security
4. Perceived Security

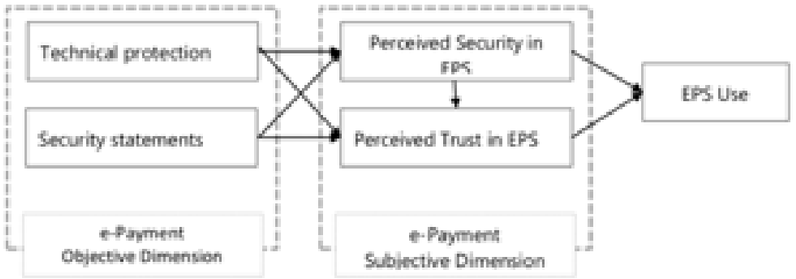
Wat we in het schema zien is dat de objectieve oftewel concrete dingen die gebruiker tegenkomt zoals de technische veiligheid (beveiligingen) en daarnaast uitspraken over hoe veilig de applicatie is. Deze twee factoren beïnvloeden hoe de veiligheid en vertrouwen wordt opgepakt door de gebruiker en resulteert in het gebruik van mobiel bankieren.

De praktische technical protection, de beveiligingen, zorgen vanzelfsprekend voor een veiliger gevoel. Echter spelen security statements en perceived trust goed in op het gevoel van veiligheid dat wordt gecreëerd door in te spelen op de doelgroep.

Security Statements

Interessant in dit schema is dat het onderdeel security statements. Volgens Mukherjee and Nath (2003) [3] is een statement over veiligheid op de website cruciaal om het gevoel van veiligheid van de consument positief te beïnvloeden. (A. de Roos &, 2011)[1]. Wanneer er mensen verteld wordt door de bank dat ze veilig zijn, gaan ze dit ook geloven. Dit kan verklaard worden door te kijken naar de principes van Cialdini die stelt dat autoriteit ervoor zorgt dat mensen dingen als waar van je aannemen op basis van de professionele positie die je hebt. (M. Segveld, 2015) [4]. Een andere security statement is het laten zien van de identiteit van de bank die wordt geverifieerd aan de gebruiker zoals verteld door Cornelis Moens van

TRUST & SECURITY MODEL



ING. Zo weten dat ze met de juiste instantie te maken hebben en wordt er een veiliger gevoel gecreëerd.

Om te bevestigen dat de banken hier gebruik van maken heb ik gekeken naar de websites van de banken waar ze de mobiele applicatie aanbieden. Hier zien we inderdaad dat bijvoorbeeld ING een statement maakt “Bankieren met uw mobiel of tablet via de Mobiel Bankieren App is veilig. Anders zouden we het niet aanbieden.”(ING, z.j.) [5] Een statement als deze verhoogt niet daadwerkelijk direct de veiligheid, maar geeft wel een gevoel van veiligheid. Soortgelijke statements vinden we ook bij vele andere banken zoals SNS bank, Rabobank en Knab.

Perceived trust

Een ander aspect wat we zien in het schema is de perceived trust. Hier gaat het om hoe de gebruiker verwacht dat de bank de transactie op een bepaalde manier laat verlopen en hoe de gebruiker deze om die reden verwacht te zien. Wanneer een transactie zonder rare handelingen gedaan kan worden en het logisch verloopt voelen mensen zich veiliger omdat het onbekend voelt voor de gebruiker.

Zelf instellen

Een geheel ander kader van de bank die je veilig laat voelen is dat de bank je de grenzen van veiligheid zelf in handen geeft. Binnen de applicatie kan namelijk naar eigen wens een daglimiet worden ingesteld waar de gebruiker zich fijn bij voelt en zeker van weet dat het zijn of rekening niet schaad mocht er iets misgaan. Ook kan de gebruiker zelf vaak instellen wat voor beveiliging hij of zij wilt gebruiken. Er kan gebruik gemaakt worden van een code, vingerafdruk enz. En de gebruiker bepaalt, in sommige gevallen ook, in welke situatie deze beveiligen gebruikt kunnen worden. In principe veranderd de sterkte van beveiliging niet heel erg, maar gaat het hierom dat de gebruiker zelf kan kiezen wat als het veiligst wordt geacht en zich daarmee het veiligst voelt.

1)De Roos, A. (2011, 12 december). Betalen met je mobiele telefoon. Geraadpleegd van http://essay.utwente.nl/61418/1/BSc_A_de_Roos.pdf

2)Kim, C., W. Tao, et al. (2010). “An empirical study of customers’ perceptions of security and trust in e-payment systems.” Electronic Commerce Research and Applications 9(1): 84-95.

3)Mukherjee, A. and P. Nath (2003). “ A model of trust in online relationship banking.”

4)Segveld, M. (2015, 13 oktober). TIJDELIJK ARTIKEL: 6 overtuigingsprincipes in de praktijk. Geraadpleegd van https://marketingmed.nl/overtuigingsprincipes-cialdini-in-de-praktijk/

5) ING Group. (z.j.). Veilig bankieren met uw mobiel of tablet. Geraadpleegd van https://www.ing.nl/de-ing/veilig-bankieren/veilig-bankzaken-regelen/veilig-bankieren-met-uw-mobiel-of-tablet/index.html

6.Welke gevoelens roept beveiliging op bij de gebruiker bij mobiel bankieren?

Arnoud Snippert, UX designer bij ING, stelde dat het lastig was om onderzoek te doen naar de gevoelens die (veiligheid bij) mobiel bankieren op doet komen. “Je merkt dat wanneer je kwalitatief onderzoek gaat doen, je vragen gaat stellen en mensen gaan doordenken, ze zich onveiliger voelen.” Dit komt omdat mensen tijdens het gebruik niet altijd bewust nadenken over de beveiliging, en pas wanneer ze geconfronteerd worden met vragen de gebruikers vraagtekens neerzetten bij de veiligheid van de applicatie. Vanuit de ING wordt gemerkt dat er dan gevoelens van onzekerheid en een onveilig gevoel bij de gebruiker komen.

Om dit te valideren zijn respondenten bij een interview/user test eerst gevraagd om gewoon door de app te navigeren en toe te lichten met daarbij wat er door ze heen ging, daarna werden vragen gesteld of de beveiliging wel genoeg was of niet. Er waren enkele positieve, negatieve en gemixte gevoelens:

Positieve gevoelens
Vooral in het geval van een extra beveiliging in de vorm van bijvoorbeeld een random reader voelen alle gebruikers zich veiliger omdat alleen zij de handeling konden uitvoeren. Bij de gebruikers van Rabobank, zoals respondent Sharon Zuidema, kwam ook zekerheid als positief gevoel naar boven, door een functionaliteit die de eigenaar van een rekening met het rekeningnummer matcht en daarmee valideert weet zij zeker dat geld overmaakt naar de juiste persoon.

Ook werd tijdens de tests duidelijk dat geen van de respondenten nadacht bij het inloggen. Hieruit bleek dat dit ook als positief werd ervaren omdat de gebruikers ervan uitgaan dat gewoon veilig is en dat ze ook met beveiliging zonder hinder kunnen inloggen.

Negatieve gevoelens
De negatieve gevoelens zijn in bijna alle gevallen situationeel. De respondenten gaven allen aan een onveilig gevoel te hebben wanneer zij zich op een onbekend netwerk netwerk begeven of zich ergerde omdat ze geen random reader bij de hand hadden.

Een ondervinding die gedaan is uit interviews met de respondenten is dat de beveiligingen zelf niet zo zeer negatieve associaties opwekken.

De user experience wordt namelijk als positief ervaren. De negativiteit van beveiliging komt voort uit de afwezigheid daarvan, zoals de random reader. Ook gaf bijvoorbeeld een respondent aan dat ze bij het overschrijven van geld een bevestiging missen dat alles goed is gelukt. Zo komt er onzekerheid naar boven of het geld wel goed is overgemaakt (naar de juiste persoon).

Gemixte gevoelens
Een interessante resultaat vanuit de respondenten is dat een identifier of random reader een veiliger gevoel gaf dan normaal, maar dat de afwezigheid daarvan niet per se minder veilig voelde. Er kwamen daarom gemixte gevoelens wat de toegevoegde waarde was van deze beveiliging is.

7.Heeft de beveiliging invloed op de user flow (het uitvoeren van taken)?

De beveiligingen die invloed uitoefenen zijn de beveiligingen waar de gebruiker zelf mee te maken heeft. Beveiligingen zoals encryptie, uitwisseling van informatie door Nederlandse vereniging van banken en een externe controle hebben geen directe invloed op het uitvoeren van taken en oefenen om die reden geen invloed uit.

De beveiligingen die wel mogelijkheid hebben tot het beïnvloeden van user flow zijn de beveiligingen waar wel mee wordt geconfronteerd. Dit zijn beveiligingen die we kunnen plaatsen onder zichtbare 'fysieke' beveiligingen en preventieve beveiligingen zoals een daglimiet of beperkte inlogpogingen.

Cornelis Moens maakte duidelijk in een interview dat ING heeft ondervonden dat een extra beveiliging zoals een reader een dip is in de user flow omdat deze niet altijd tot je beschikking en voor extra handelingen zorgt. Dit werd bevestigd door de meerdere respondenten. Bij verdieping op dit probleem kan er gesteld worden dat dit niet aan de beveiliging maar aan de afwezigheid daarvan. Sharon Zuidema vertelde zo dat ze vroeger de reader voor elke transactie nodig had. Dit zorgde ervoor dat ze hem altijd bij zich had. Tegenwoordig is echter alleen nog maar nodig bij een overschrijving van een groot bedrag of onbekend persoon. Meerdere banken zijn overgestapt naar een gebruiksvriendelijker systeem waarbij de reader niet altijd nodig. (D. Vleugel, 2017) (Dit zorgde er echter voor dat mensen de reader niet meer altijd bij zich hadden. Hoewel de user experience dus wellicht beter werd op de applicatie, komt er door situationeel gebruik van een random reader een grotere dip in de user flow.

Positieve invloed
Doorgaans was vanuit de respondenten gebleken dat de gebruikers geen hinder ondervinden van de beveiligen. De beveiligen zijn in de meeste gevallen completentair aan de user experience omdat de gebruiker zo het idee heeft dat ze geen foute handelingen maken en veel zekerheid hebben tijdens het uitvoeren taken. Dat het gebruik met beveiligingen positieve invloed heeft te maken met verschillende factoren: De gebruiker wordt verteld dat het veilig is, ze moeten een aparte code ontvangen om de app te activeren, ze zetten zelf grenzen en voorkeuren voor beveiligen en doen het alleen op netwerk dat ze vertrouwen. Deze factoren maken dat de gebruiker zich veilig voelt en zich ook niet zo snel hindert aan de beveiligen die worden voorgelegd.

Vleugel, D. (2017, 18 december). Update ABN AMRO-app: betalingen bevestigen met je smartphone. Geraadpleegd van https://androidworld.nl/apps/abn-amro-betalingen-bevestigen-smartphone/

Vleugel, D. (2017, 19 december). KNAB maakt cardreader overbodig door gebruik van smartphone bij betalingen. Geraadpleegd van https://androidworld.nl/apps/knab-bank-bevestigen-betaling-app/

8. Conclusie

Op welke manier heeft veiligheid invloed op de user experience bij mobiel bankieren?

In de hypothese werd verondersteld dat beveiligingen als hinderlijk ervaren konden worden omdat ze een obstakel waren bij het direct uitvoeren van taken. Echter is doorgaans gebleken dat de beveiligingen en het proces dat de gebruiker doorloopt om tot de applicatie te komen complementair is aan de user experience. De beveilingen hebben positieve invloed in de zin dat ze veiligheid bieden en de gebruiker zich op zijn gemak stelt omdat ze naar eigen voorkeur de beveiligingen implementeren in de applicatie. Daarnaast zijn door de bank gegeven veiligheidsstatements ten goede van de user experience omdat er zo vertrouwen wordt gewekt bij de doelgroep. De enige manier waarop veiligheid invloed heeft is situationeel. Namelijk bij de afwezigheid van een veilig netwerk of een random reader (of soortgelijk apparaat.)

9. Literatuur

1) Redactie Emerce. (2017, 22 februari). 'Nederlanders nemen het voortouw bij het internet-bankieren'. Geraadpleegd van https://www.emerce.nl/nieuws/nederlanders-nemen-voortouw-internetbankieren

2)ING Group. (z.j.). Feiten en Cijfers. Geraadpleegd van https://www.ing.nl/nieuws/feiten_en_cijfers/index.html

1)De Roos, A. (2011, 12 december). Betalen met je mobiele telefoon. Geraadpleegd van http://essay.utwente.nl/61418/1/BSc_A_de_Roos.pdf

2)Kim, C., W. Tao, et al. (2010). "An empirical study of customers' perceptions of security and trust
in e-payment systems." Electronic Commerce Research and Applications 9(1): 84-95.

3)Mukherjee, A. and P. Nath (2003). " A model of trust in online relationship banking."

4)Segveld, M. (2015, 13 oktober). TIJDELIJK ARTIKEL: 6 overtuigingsprincipes in de praktijk. Geraadpleegd van https://marketingmed.nl/overtuigingsprincipes-cialdini-in-de-praktijk/

5) ING Group. (z.j.). Veilig bankieren met uw mobiel of tablet. Geraadpleegd van https://www.ing.nl/de-ing/veilig-bankieren/veilig-bankzaken-regelen/veilig-bankieren-met-uw-mobiel-of-tablet/index.html

Vleugel, D. (2017, 18 december). Update ABN AMRO-app: betalingen bevestigen met je smartphone. Geraadpleegd van https://androidworld.nl/apps/abn-amro-betalingen-bevestigen-smartphone/

Vleugel, D. (2017, 19 december). KNAB maakt cardreader overbodig door gebruik van smartphone bij betalingen. Geraadpleegd van https://androidworld.nl/apps/knab-bank-bevestigen-betaling-app/

Met dank aan de respondenten:

Sharon Zuidema
Iris de Lang
Malou van Rennes
Skip Overeem
Yien Wei Thye

Cornelis Moens, ING
Arnoud Snippert, ING