Defence, Safety & Security
Kampweg 55
3769 DE Soesterberg
Postbus 23
3769 ZG Soesterberg

www.tno.nl

T +31 88 866 15 00
F +31 34 635 39 77

TNO-rapport

TNO 2018 R11330

De menselijke kant van cybersecurity: Conceptuele ontwikkelingen en de Cyber Security Assistent

Datum	november 2018
Auteur(s)	M. Roelofs, MSc Drs. N.M. de Koning Dr. A.J. van Vliet Dr. R. Wijn Drs. R. van Rijk Dr. H.J. Young
Oplage	n.v.t.
Aantal pagina's	93 (incl. bijlagen)
Aantal bijlagen	2
Opdrachtgever	A.C. Kernkamp (Programmaleider VP Cyber 2018 - P102) met projectbegeleiding door D. van Luijk (Ministerie van Justitie & Veiligheid, NCSC)
Projectnaam	Cyberveiligheid Gedragsinterventies
Projectnummer	060.31921/01.10

Inhoudsopgave

Bijlage(n)

A Overzicht onveilige cybergedragingen en interventies
B Design Patterns

Samenvatting

Sinds een aantal jaar doet TNO onderzoek naar human factors in cybersecurity. Deze onderzoekslijn richt zich op cyber onveilig gedrag van mensen.
Wij onderzoeken de redenen en de totstandkoming van cyber(on)veilig gedrag en ontwikkelen een kader voor het identificeren van interventies om cyberveilig gedrag te stimuleren.
Het werk in deze onderzoekslijn focust zich op cyberveilig gedrag van bedrijfsmedewerkers. Wij richten ons op het geven van adviezen over hoe cyberveilig gedrag van medewerkers te vergroten aan diegenen die binnen hun organisatie verantwoordelijk zijn voor cybersecurity. Denk aan CISO's, securitymanagers, lijnmanagers enzovoorts.
In het kort betreft cybergedrag de activiteiten die mensen in de online/digitale omgeving uitvoeren en hoe ze deze uitvoeren. Voorbeelden van activiteiten zijn bijvoorbeeld het surfen op het Internet, e-mailen of streamen. De middelen die mensen gebruiken om deze activiteiten uit te voeren (de *hoe*-vraag) zijn bijvoorbeeld publieke draadloze netwerken, cloud diensten voor opslag of informatieoverdracht, of torrentdiensten voor het downloaden van bestanden.
Veel cyberactiviteiten kunnen risico's met zich meebrengen. Er is altijd een kans dat anderen meekijken, malware of ransomware ongewenst op een device worden geïnstalleerd, of gegevens worden gestolen.
Het werk dat in dit rapport wordt beschreven richt zich op de volgende onderzoeksvragen:

1 Waarom vertonen mensen onveilig cybergedrag en welke aanknopingspunten zijn er om cyberveilig gedrag te faciliteren?
2 Hoe kunnen diegenen, die binnen organisaties verantwoordelijk zijn voor cyberveiligheid, ondersteund worden in dit proces?

Doelstelling van dit rapport is om een overzicht te geven van de activiteiten die in de eerste helft van 2018 zijn uitgevoerd om antwoord te geven op de onderzoeksvragen.
Het belangrijkste resultaat van dit werk is de Cyber Security Assisstant (CSA). De CSA is een digitale tool die de gebruiker helpt cyberonveilig gedrag beter te begrijpen langs de lijnen van onze conceptuele visie. Daarnaast geeft de CSA een overzicht van verschillende geschikte interventies om cyberveilig gedrag te vergroten.
Het rapport kent drie delen.

DEEL 1 CONCEPTUELE DOORONTWIKKELING

In dit deel bespreken wij een visie op het veranderen van (cyber)gedrag en beschrijven een taxonomie van slachtofferschap, risicovolle cybergedragingen en psychologische processen die daaraan ten grondslag liggen.
Cybergedrag (bijvoorbeeld gebruik maken van een openbare WiFi) is meestal een middel om een persoonlijk doel (bijvoorbeeld mail doorlezen) te bewerkstelligen. Cybergedrag is doorgaans geen doel op zich. Om cyberveilig gedrag te vergroten, lijkt het effectiever te zijn om het doel van mensen te identificeren en ervoor te zorgen dat mensen het doel kunnen nastreven op een cyberveilige manier. Kortom: cyberrisico's verkleinen door het cybergedrag van mensen te faciliteren in plaats van te frustreren.

In het kort stellen wij dat het veiliger maken van cybergedrag niet gaat via het bewust willen veranderen van gedrag omdat dit eerder tot frustratie en omwegen zal leiden. In plaats daarvan stellen wij voor om na te gaan waarom mensen onveilig gedrag vertonen – zoek naar hun onderliggende doelen – en om die doelen op een cyberveilige manier te faciliteren.
De beschreven taxonomie over slachtoffergedrag begint bij slachtoffers van cybercrime en gaat in op vier elementen van hun onveilige cybergedrag die belangrijk zijn in het verklaren en voorkomen daarvan: gedragsdoelen, risicogedragingen, psychologische processen en informatieverwerking.

Deel 2 Activiteiten

In dit deel beschrijven wij de activiteiten die wij hebben uitgevoerd in het ontwikkelproces dat heeft geleid tot de Cyber Security Assistant (CSA). In eerste instantie is gekeken naar het gebruik van *design patterns* om interventies te categoriseren en inzichtelijke te maken voor de gebruiker, waardoor de interventiekeuze gefaciliteerd wordt. Uiteindelijk is deze aanpak niet gebruikt in de CSA omdat veel design patterns een inhiberende insteek hebben in het veranderen van gedrag, terwijl onze conceptuele visie gebaseerd is op het mogelijk maken (faciliteren) van gedrag.
Interviews met potentiele eindgebruikers van de CSA zijn gehouden om inzicht te krijgen in hun ondersteuningsbehoeften: hoe zouden ze een ondersteunende tool gebruiken, wat hebben ze nodig om ondersteuning in hun organisatie te laten landen, etc. Geïnterviewden waren veelal positief over de CSA en zien het als een handige tool voor o.a. de afdelingen die zich bezig houden met het managen van de cyber security risico's. De geïnterviewden zagen veel toepassingen, zoals helpen bij verantwoording naar hoger management, ondersteuning bij de analysefase en stimuleren van de variatie waarmee cybersecurity risico's worden aangepakt. Ook kwamen veel aanbevelingen voor functionaliteiten uit de interviews zoals goede zoekfunctie, logfunctie, output over KPI's en effectmetingen, en dat het aan te passen is aan de eigen organisatie.

Deel 3 Tools, ondersteuning en evaluatie

De CSA is een digitale tool die op een gestructureerde manier ondersteunt bij de gedragsanalyse van cyber onveilig gedrag. Vervolgens helpt de CSA het gedrag te koppelen aan passende en concrete cybersecurity oplossingen oftewel interventies te komen. De CSA is bedoeld voor mensen die de taak hebben cybersecurity binnen bedrijven te vergoten, handhaven en monitoren, en die geen achtergrond hebben in de sociale wetenschappen.
Om cyberveiligheid te beoordelen is het belangrijk om vast te stellen wat het niveau is van de subjectieve beleving van cyberveiligheid. Hiertoe is de cyber security monitor ontwikkeld. Idealiter wordt dit aangevuld met KPI's die iets zeggen over het objectieve niveau van cyberveiligheid. Dit kan gemeten worden via bijvoorbeeld tellingen of logging van systeeminformatie. Van uiterst belang bij het verkrijgen van inzicht in het niveau van cyberveiligheid is het idee dat het gaat om het meten van veranderingen. Daarom bevelen wij aan de KPI's periodiek te meten, bijvoorbeeld ieder jaar. Alleen dan is het mogelijk om iets te zeggen over van cyberveiligheid op een overkoepelend niveau en over de effecten die interventies teweeg brengen op concreet niveau.

De CSA en effectmetingsmethodiek zijn in de workshop Veilig Werken geëvalueerd met stakeholders van verschillende organisaties. Ook is daar een vragenlijst uitgezet over cyberproblematiek. De resultaten van de workshop bevestigden de inzichten verkregen uit de interviews. Uit de vragenlijst blijkt dat men goed in staat is om de redenen te noemen waarom mensen zich cyberonveilig gedragen. Men is echter niet goed in staat om daar gevarieerde interventies aan te koppelen: awareness verhogen en technische oplossingen zoals filters, zwaaien nog steeds de scepter. Samengenomen, onderschrijft dit de noodzaak om op een andere manier over cyberveiligheid na te denken, namelijk vanuit het doel van de gebruiker en hoe de gebruiker via praktische, faciliterende interventies cyberveilig ondersteund kan worden.

1 Inleiding

Sinds een aantal jaar doet TNO onderzoek naar human factors in cybersecurity. Deze onderzoekslijn richt zich op cyber onveilig gedrag van mensen. Wij onderzoeken de redenen en de totstandkoming van cyber(on)veilig gedrag en ontwikkelen een kader voor het identificeren van interventies om cyberveilig gedrag te stimuleren. De wetenschappelijke basis voor dit onderzoek ligt in de sociale psychologie, maar in de projecten maken we gebruik van een aanpak waarin ook de vakgebieden onderwijskunde en omgevingspsychologie zijn meegenomen.
Het werk in deze onderzoekslijn focust zich op cyberveilig gedrag van bedrijfs-medewerkers. Wij richten ons op het geven van adviezen over hoe cyberveilig gedrag van medewerkers te vergroten aan diegenen die binnen hun organisatie verantwoordelijk zijn voor cybersecurity. Denk aan CSIO's, securitymanagers, lijnmanagers enzovoorts.
In het kort betreft cybergedrag de activiteiten die mensen in de online/digitale omgeving uitvoeren en hoe ze deze uitvoeren. Voorbeelden van activiteiten zijn bijvoorbeeld het surfen op het Internet, emailen of streamen. De middelen die mensen gebruiken om deze activiteiten uit te voeren (de *hoe*-vraag) zijn bijvoorbeeld publieke wireless netwerken, cloud services voor opslag of informatietransfer, of torrentdiensten voor het downloaden van bestanden.
Veel cyberactiviteiten kunnen risico's met zich meebrengen. Er is altijd een kans dat anderen meekijken, malware of ransomware ongewenst op een device worden geïnstalleerd, of gegevens worden gestolen.
Cyberveilig gedrag doelt op het uitvoeren van activiteiten in de digitale wereld op een manier waardoor mogelijke risico's worden verkleind. Onveilig cybergedrag doelt op het uitvoeren van digitale activiteiten op een manier waardoor de gebruiker vatbaarder is voor cyberdreigingen.
In 2016/2017 lag de focus van ons onderzoek op het begrijpen van de onderliggende gedragsprocessen bij cybergedrag. Dit resulteerde in het TNO cybersecurity framework. Dit framework beschrijft drie paden waarlangs (cyber)gedrag tot stand kan komen: reflexmatig, gewoontematig of weloverwogen. Onderdelen van dit framework zijn bij twee grote Nederlandse organisaties getest met als use case het klikken op en melden van phishing mail, en wachtwoordbeheer.
In 2018 is de focus enerzijds het door ontwikkelen van onze conceptuele visie op het veranderen van cybergedrag en anderzijds het ontsluiten van deze kennis opdat anderen, zonder uitgebreide kennis van de sociale wetenschappen, onze visie kunnen begrijpen en zelf kunnen toepassen in hun eigen organisatie, om cyberveilig gedrag te vergroten .
Het ontsluiten gebeurt middels de volgende activiteiten:

- Het ontwikkelen van de Cyber Security Assistent (CSA). Dit is een prototype waarmee gebruikers inzicht krijgen in het cybergedrag van hun medewerkers dat ze willen veranderen en bijpassende interventies. Ook geeft de CSA inzicht in hoe men een effect van een interventie meetbaar kan maken.
- Het uitvoeren van een beproeving bij een groot Nederlands particulier bedrijf.[1] Hierin wordt met het bedrijf de bruikbaarheid van de CSA op de proef gesteld.
- Disseminatie. In 2018 ligt er een nadrukkelijke focus op *stakeholder engagement* via interviews, workshops, publicaties en presentaties.

[1] Om privacy redenen wordt de deelnemende bedrijf niet geïdentificeerd.

1.1.1 Doelstelling en onderzoeksvragen

Het werk in de eerste helft van 2018 richt zich op de volgende onderzoeksvragen:

1 Waarom vertonen mensen onveilig cybergedrag en welke aanknopingspunten zijn er om cyberveilig gedrag te faciliteren?
2 Hoe kunnen diegenen die binnen organisaties verantwoordelijk voor cyberveiligheid ondersteund worden in dit proces?

Doelstelling van dit rapport is om een overzicht te geven van de activiteiten die in de eerste helft van 2018 zijn uitgevoerd om antwoord te geven op de onderzoeksvragen. Wij hebben getracht de volgorde en beschrijving van deze activiteiten een logische opbouw te geven om leesbaarheid van het rapport te vergroten. Wij adviseren de lezer echter te onthouden dat dit rapport met name een vastlegging en opsomming betreft van deze activiteiten in tegenstelling tot een integratie.

1.1.2 Leeswijzer

Dit rapport is verdeeld in drie delen. In het eerste deel, *Conceptuele doorontwikkeling*, beschrijven wij in Hoofdstuk 2 de ontwikkelingen van onze conceptuele ideeën over hoe gedrag effectief veranderd kan worden. In Hoofdstuk 3 beschrijven wij een inventarisatie van risicovolle cybergedragingen, achterliggende psychologische antecedenten en passende interventies, met als doel het opstellen van een taxonomie van slachtoffergedrag.
In het tweede deel, *Activiteiten*, beschrijven wij de activiteiten die wij hebben uitgevoerd in het ontwikkelproces dat heeft geleid tot de Cyber Security Assistant (CSA). In Hoofdstuk 4 bespreken wij *design patterns* en hun potentiële toepassing bij het beïnvloeden van cybergedrag.[2] Hoofdstuk 5 beschrijft interviews die zijn uitgevoerd met stakeholders om inzicht te krijgen in hun ondersteuningsbehoeften: hoe zouden ze een ondersteunende tool gebruiken, wat hebben ze nodig om ondersteuning in hun organisatie te laten landen, etc.
In het derde deel, *Tools, ondersteuning en evaluatie*, beschrijven wij in Hoofdstuk 6 de CSA, een tool om stakeholders te helpen onveilig cybergedrag inzichtelijk te maken en te ondersteunen bij het kiezen van een gepaste interventie. Hierin beschrijven wij de tool, voor wie deze bedoeld is en hoe deze gebruikt kan worden. Hoofdstuk 7 blikt vooruit naar een volgende stap in de ontwikkeling van de CSA, namelijk de inclusie van informatie over effectmetingen en Key Performance Indicators (KPI's). Hoofdstuk 8 doet verslag van de Workshop Veilig Werken waarin wij de CSA met een aantal stakeholders hebben geëvalueerd. Ook wordt daar een vragenlijst over cyberproblematiek besproken.
Hoofdstuk 9 zet tot slot de belangrijkste conclusies op een rij, vat de antwoorden op de onderzoeksvragen samen, en kijkt vooruit naar het werk in de tweede helft van 2018.

[2] *Design patterns* zijn een soort sjablonen voor het sturen van menselijk gedrag, door de manier waarop je de tools, die mensen gebruiken voor hun gedrag, ontwerpt.

Deel I: Conceptuele doorontwikkeling

In 2018 is onze conceptuele begrip van cybergedrag en het veranderen ervan ontwikkeld op twee gebieden die in Deel 1 van dit rapport besproken worden:

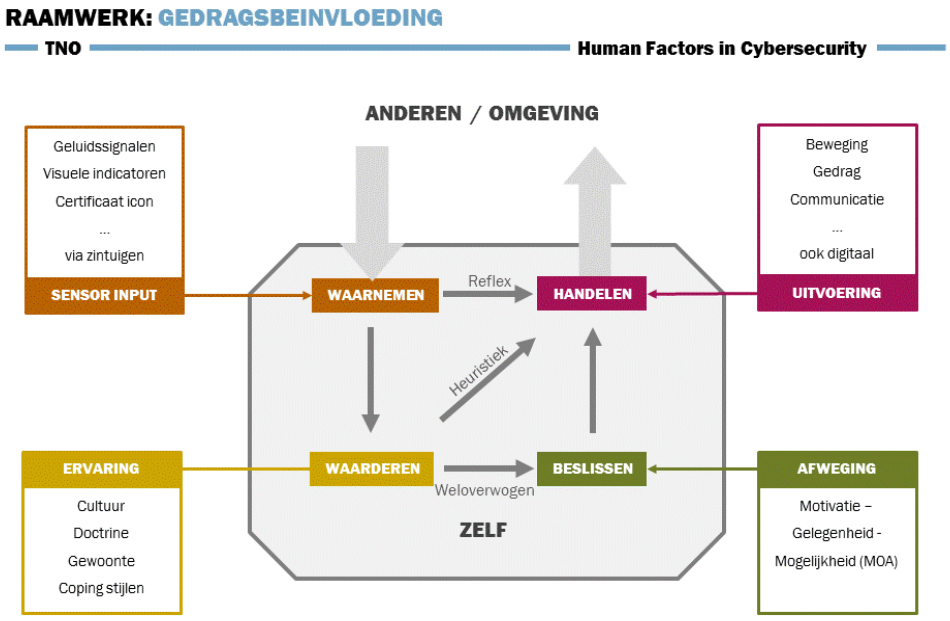
1 Beter begrip waarom mensen onveilig handelen en hoe daarop ingegrepen kan worden (Hoofdstuk 2).
2 Beter overzicht van cybergedrag in termen van informatieverwerkingsprocessen, onderliggende psychologische processen, risicogedragingen en gedragsdoelen (Hoofdstuk 3).

2 Effectief veranderen van gedrag[3]

De concepten die wij in 2016 en 2017 hebben ontwikkeld worden in 2018 doorontwikkeld om steeds meer begrip te krijgen van menselijk gedrag in de digitale wereld. In ons eerder werk lag de focus op hoe gedrag tot stand komt en resulteerde in de TNO Cybersecurity Framework (Paragraaf 2.1.1). In 2018 is de focus met name op het kiezen van interventies om mensen aan te sporen cyberveiliger te handelen. Het werk dat in dit hoofdstuk wordt beschreven tracht antwoord te geven op de eerste onderzoeksvraag, namelijk*: Waarom vertonen mensen onveilig cybergedrag en welke aanknopingspunten zijn er om cyberveilig gedrag te faciliteren?*

2.1.1 TNO Cybersecurity Framework

In 2016 en 2017 was de focus van ons denken met name gericht op de totstandkoming van cyber onveilig gedrag en het onderscheiden van verschillende soorten gedragingen. Dit leidde tot het TNO Cybersecurity Framework (van Vliet, 2017; zie Figuur 2-1).



Figuur 2-1 TNO Cybersecurity Framework.

Samengevat is het framework als volgt. Op het gebied van menselijk gedrag in cybersecurity, staat centraal dat er drie paden zijn waarlangs gedrag tot stand komt. Deze staan hier afgebeeld en zijn gebaseerd op de stappen in de OODA loop (Observe, Orient, Decide, Act).
Het gedrag zelf staat rechtsboven: *Act*. Wanneer de situatie een handeling (gedrag) vereist, is de eerste mogelijkheid *Observe*. Informatie komt binnen, er is een kant en klare bijpassende handeling die zonder verder cognitieve verwerking wordt uitgevoerd. Dit is nagenoeg een stimulus-respons handeling: reflexmatig.

[3] Delen van Hoofdstuk 2 zijn gereproduceerd uit een artikel in het tijdschrift *Beveiliging* (zie Young et al., 2018; https://view.publitas.com/security-press/beveiliging-april-2018).

Een voorbeeld is als je voorligger op de snelweg hard op zijn rem trapt, doe jij dat ook.
De tweede mogelijkheid is dat een reflexieve handeling niet volstaat; er moet over het uit te voeren gedrag worden nagedacht: *Appraise*. Gelukkig is de situatie bekend en is een geschikt gedrag voor handen. Een voorbeeld is het kiezen van wat je 's ochtends aantrekt. Het gaat zeker niet reflexmatig, maar je hoeft er niet echt veel over na te denken. In deze categorie vallen gewoontes, oftewel gedrag dat door heuristieken wordt aangestuurd.
De laatste verwerkingsmogelijkheid treedt op wanneer dat wat gevraagd wordt niet via een reflex kan, er geen gewoontes of heuristieken voor zijn, en het gevraagde belangrijk is. In dit geval zijn mensen gemotiveerd om een goed passend gedragsrespons te vinden. Schaarse cognitieve middelen worden aangewend en het gedrag komt via een bewuste *Decide* route tot stand. Voorbeeld is het afsluiten van een hypotheek. Je wilt de juiste en beste hypotheek voor jou en om dit te doen, moet je de alternatieven afwegen en een geïnformeerde keuze maken.

2.1.2 Interventies voor cyberveilig gedrag

In de doorontwikkeling van het framework is de focus komen te liggen op interventies voor het effectief ingrijpen op de verschillende gedragssoorten.
Met name het veranderen van gewoontegedrag is een interessante uitdaging.
Tot nu toe wordt veelal geïntervenieerd op gewoontegedag via het verhogen van cyberawareness. Maar men komt steeds meer tot de conclusie dat het verhogen van het bewust zijn van dreigingen, risico's, consequenties en wat men wél zou moeten doen niet tot blijvende gedragsverandering leidt (Bada, Sasse & Nurse, 2014).
Een voorbeeld om dit te verduidelijken. Veel mensen weten dat ze 250 gram groente per dag moeten eten, maar slechts 2% van de Nederlandse bevolking haalt dat (RTL Nieuws, 2016). Mensen kennen de richtlijnen, ze kennen de gezondheids-voordelen en groente is beschikbaar en betaalbaar. Awareness is dus best op orde maar het gedrag (250 gram groente eten per dag) komt niet tot stand. Een conclusie lijkt daarmee vanzelfsprekend: het eten van groente heeft weinig te maken met awareness.
Een belangrijke reden waarom awareness creëren slechts matig werkt, is waarschijnlijk dat awareness wordt ingezet om gedrag, wat mensen wel graag willen doen, te veranderen of te verbieden. Zo is het bijvoorbeeld aannemelijk dat de beslissing om openbare WiFi in de trein wel of niet te gebruiken niet makkelijk beïnvloed zal worden door mensen enkel bewust te maken van de risico's.
Het nastreven van hun doel (bijvoorbeeld emaillen, websurfen, streamen, of gewoon altijd bereikbaar zijn) zal vaak zwaarder wegen als er geen voor de hand liggend alternatief is.
Het idee dat awareness niet altijd leidt tot cyberveilig gedrag past ook in het Cybersecurity Framework. Bij gewoontegedrag gaat het erom dat je onbewust inschat of er sprake is van een onbekende of onverwachte situatie waarbij je huidige gewoonte niet volstaat. Als de situatie bekend en verwacht is, is het *business as usual* en volstaan je normale gewoonten; je doet dan wat je altijd doet. Dit vinden mensen over het algemeen ook het prettigst. Indien er wel sprake is van een onbekende of onverwachte situatie, gaat men op zoek naar ander gedrag. Dit is soms makkelijk, maar soms lastig of vervelend.
Als iemand continu of herhaaldelijk uitgedaagd wordt om alternatief gedrag te zoeken, waardoor iemand regelmatig belemmerd wordt in zijn/haar doen en laten, en het alternatief is lastig of vervelend, leidt dit tot frustratie. Om een eind te maken

aan deze onwenselijke staat, vallen mensen uiteindelijk terug in oude gewoontes. Hierbij wegen de nadelen van de alternatieven (bijvoorbeeld kost te veel moeite, ik krijg het niet onder de knie, maakt wat ik wil onmogelijk) zwaarder dan de nadelen van de oude gewoontes (is niet cyberveilig).
Als we het bovenstaande toepassen op het eerdere voorbeeld van het gebruik van openbare WiFi, zou de situatie er als volgt uit kunnen zien:

> Je zit na je werk in de trein op weg naar huis en wilt daar zoals gewoonlijk je e-mail nog even bijwerken op je laptop (je gewoonte). Je hebt laatst via je werk echter voorlichting gekregen over hoe gevaarlijk het gebruik van openbare WiFi is (nadelen van de gewoonte). Je neemt je voor om WiFi in de trein niet meer te gebruiken en zoekt een alternatief (onbekende situatie). Je nieuwe plan is om je e-mail 's avonds te doen (alternatief gedrag). Helaas geeft dit weer andere problemen: de kinderen willen je aandacht, je moet tennissen, je bent moe, het kost je het grootste deel van je avond of je hebt simpelweg geen zin in werk na het eten (nadelen van het alternatief). Dit is dus geen bevredigende oplossing, maar als je je mail niet doet, heb je de volgende dag een uitpuilende inbox. In combinatie, leiden de nadelen van het alternatief gedrag tot irritatie en frustratie. Op den duur is de kans dus groot dat je ondanks wat je geleerd hebt over het risico van openbare WiFi, je toch maar de stoute schoenen aantrekt en gewoon weer op Internet in de trein zit. En trouwens, het heeft in het verleden nooit problemen opgeleverd dus het risico zal wel meevallen…

Wil je als werkgever dat mensen niet op openbaar WiFi werken, dan moet je het omdraaien. Vraag niet van medewerkers dat ze op een andere wijze hun werk inrichten (zich op een andere manier moeten gedragen), maar kijk hoe je hun normale werkwijze cyberveilig kunt faciliteren. In het licht van bovenstaand voorbeeld: zorg ervoor dat je medewerkers gewoon in het openbaar kunnen werken, maar dan op een veilige manier. Geef ze een dongel, laat ze hun mobiel als hotspot gebruiken of voer het gebruik van VPN's in. Deze opties kosten de werknemer weinig extra moeite in vergelijking met de openbare WiFi – en zeker in vergelijking met het zoeken naar een nieuwe gedrag – en zijn een stuk veiliger.

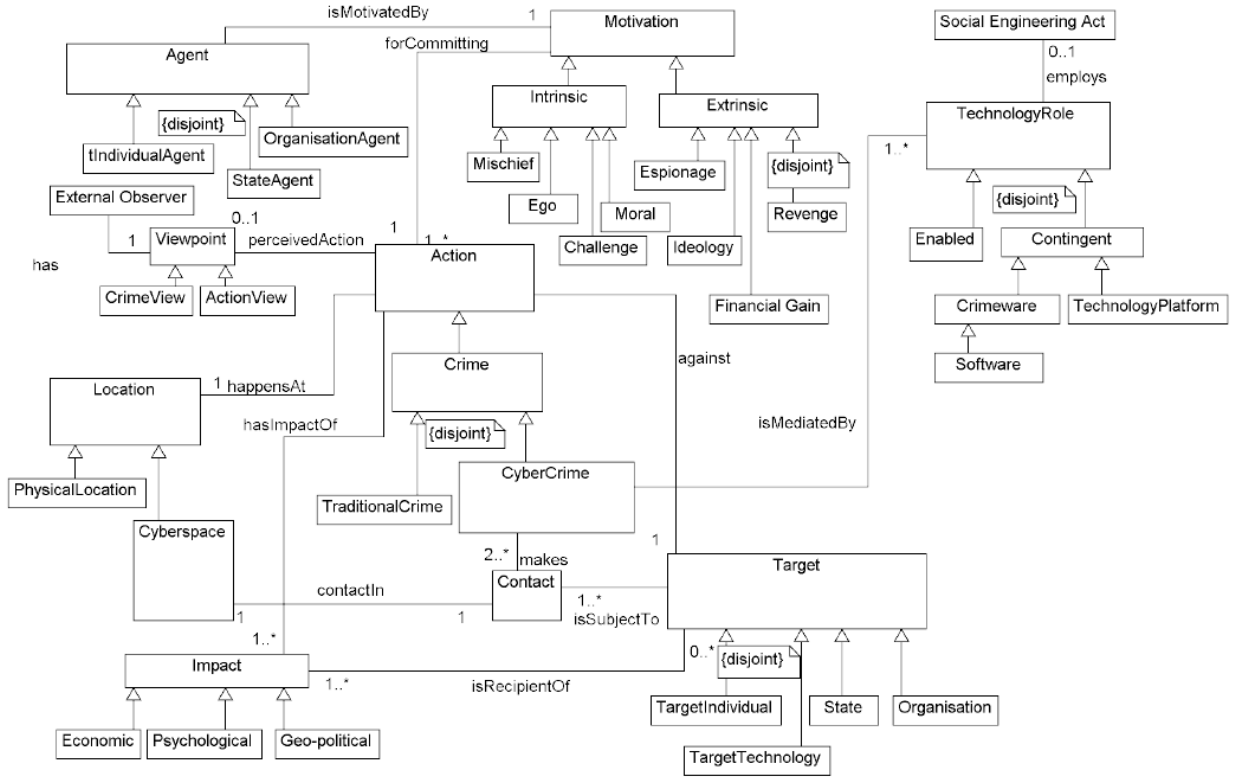
2.1.3 Samengevat

Cybergedrag (bijvoorbeeld gebruik maken van een openbare WiFi) is meestal een middel om een persoonlijk doel (bijvoorbeeld mail doorlezen) te bewerkstelligen. Cybergedrag is doorgaans geen doel op zich. Om cyberveilig gedrag te vergroten, lijkt het effectiever te zijn om het doel van mensen te identificeren en ervoor te zorgen dat mensen het doel kunnen nastreven op een cyberveilige manier. Kortom: cyberrisico's verkleinen door het cybergedrag van mensen te faciliteren in plaats van te frustreren.
In het kort stellen wij dat het veiliger maken van cybergedrag niet gaat via het bewust willen veranderen van gedrag omdat dit eerder tot frustratie en omwegen zal leiden. In plaats daarvan stellen wij voor om na te gaan waarom mensen onveilig gedrag vertonen – zoek naar hun onderliggende doelen – en om die doelen op een cyberveilige manier te faciliteren.

3 Taxonomie van cybergedrag

Bij elke cyberaanval zijn daders betrokken, met hun kwaadaardige doelen en middelen; en slachtoffers, met hun doelen en risicovolle gedragingen. In dit hoofdstuk is hiervoor relevante aspecten in kaart gebracht door een scala aan factoren die gerelateerd zijn aan cyberaanvallen en cybersecurity in het algemeen, zoals type dader, aanvalskenmerken, en risicogedrag geïnventariseerd. Deze aspecten zijn zowel onafhankelijk van elkaar onderzocht. Daarnaast zijn deze aspecten ook in samenhang beschouwd, wat om twee redenen belangrijk is.
De eerste reden heeft te maken met de kosten van de gevolgen van cybercrime. Er is een aardig goed inzicht in de kosten die gepaard gaan met specifieke typen online criminaliteit. Bijvoorbeeld, de schade door phishing mails wordt geschat op ca 150.000 euro per jaar voor middelgrote bedrijven (Ponemon, 2017). Er zijn ook beelden over type daders en hun doelen (bijvoorbeeld, verzenders van phishing mails hebben nauwelijks technische kennis of vaardigheden nodig en financiële winst is hun enige of voornaamste drijfveer). Maar kennis over hoe mensen slachtoffer worden van dergelijke criminaliteit beperkt zich nog grotendeels tot de gedragsobservatie dat slachtoffers links in phishing mails openen. Er is geen systematiek in onderzoek naar hoe doelen van daders zich verhouden tot gedrag van slachtoffers, laat staan hoe doelen van daders zich verhouden tot de redenen voor het gedrag van slachtoffers. Het gevolg is dat het deel van gedragingen waar individuen en organisaties invloed op hebben onvoldoende benut worden. Dus om de kosten van risicovol gedrag en de redenen voor het vertonen van dit gedrag te kunnen kwantificeren moeten daders en slachtoffers en hun doelen en gedragingen in samenhang bekeken worden.
De tweede reden om daders en slachtoffers in samenhang te beschouwen is om een systematisch onderzoeksagenda te kunnen opstellen. Op dit moment lijkt onderzoek naar risicogedrag, de antecedenten van dat gedrag (inclusief doelen die mensen met hun gedrag proberen te bereiken) en interventies om die gedragingen te veranderen, ad hoc tot stand te komen. Onderzoeksvragen lijken vooral gebaseerd te zijn op de expertise en interesse van onderzoekers en onderzoeksgroepen en in mindere mate op een systematische analyse van de verschillende risicovolle cybergedragingen en antecedenten. In een poging om die leemte te vullen hebben we eerder een cyber security framework (van Vliet et al., 2017; Paragraaf 2.1.1), ontwikkeld. Op basis van die framework hebben we een inventarisatie gemaakt van attitudes, heuristieken en andere cognitieve processen die ertoe kunnen leiden dat mensen risicovol gedrag vertonen.
De samenhang tussen onderdelen van een cyberaanval komt onder andere tot uiting in taxonomieën, waarin beoogd wordt die onderdelen hiërarchisch te ordenen. Diverse auteurs hebben meer of minder uitgebreide taxonomieën van cybercrime gemaakt en daarbij verschillende elementen van een cybercrime uitgelicht. Suleman (2016) maakt bijvoorbeeld een onderscheid tussen socio-economisch (gericht op financieel gewin), psychosociale (gericht op hedonistische motieven of op het aanbrengen van schade aan individuen) en geopolitisch (vaak ideologisch of idealistisch) doelen van daders, en deelt langs die groepen verschillende cyberdelicten in. Sabillon, Crano, Cavaller en Serra (2016) hebben juist geprobeerd met hun categorieën uitputtende lijsten te maken. Hun taxonomie bevat 14 typen daders, 14 doelen, 63 aanvalskenmerken en 27 typen cyberdelicten. Barn en Barn (2016) merken op dat veel taxonomieën beschrijvend van aard zijn, wat leidt tot incompleetheid en ambiguïteit. De auteurs proberen met een semi-formele benadering meer structuur te brengen in een taxonomie. Een van de

resultaten van hun bendering is Figuur 3-1, waarin ook een aantal van de eerdergenoemde taxonomieën, of delen daarvan, is verwerkt.



Figuur 3-1 Taxonomy Barn en Barn (2016).

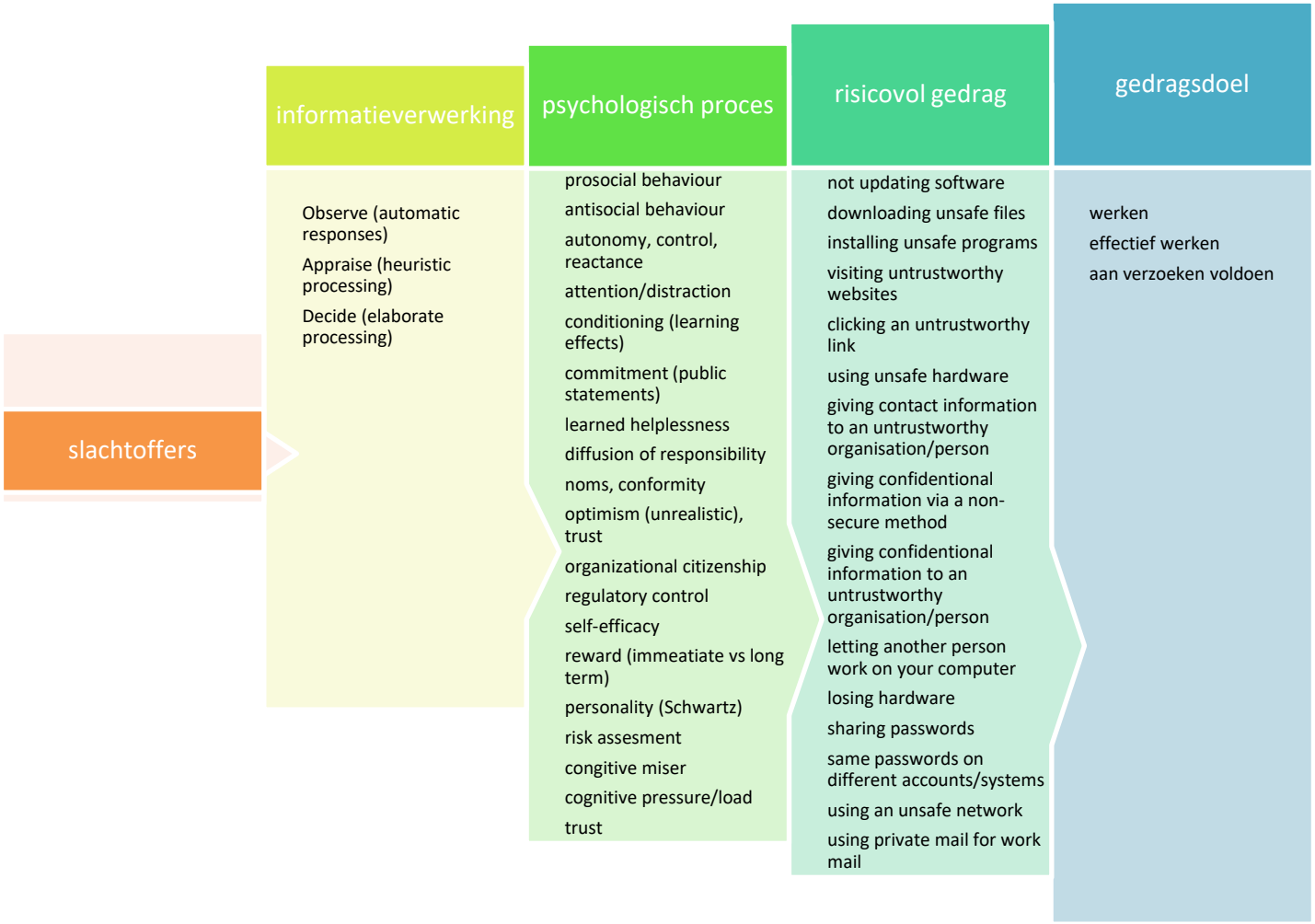
In de bestaande taxonomieën ligt de focus vaak nadrukkelijk op het delict, de gebruikte middelen en de daders. Minder belicht is de kant van risicogedrag dat tot slachtofferschap kan leiden. Op basis van ons onderzoek doen we derhalve een poging om daar meer licht op te laten schijnen. We beschrijven daarom hier niet uitgebreid de daderkant in de taxonomie maar focussen op de risicogedragingen die tot slachtofferschap kunnen leiden.

De uit deze analyse resulterende taxonomie (zie Figuur 3-1) begint bij slachtoffers en gaat in op vier elementen van hun onveilige cybergedrag die belangrijk zijn in het verklaren en voorkomen daarvan: gedragsdoelen, risicogedragingen, psychologische processen en informatieverwerking.

Mensen vertonen doelgericht gedrag, ook de slachtoffers van cybercrime. Gedrag is dus een middel om, meer of minder bewust, een doel te bereiken. Een doel kan chronisch aanwezig zijn of ontstaan door interne of externe veranderende omstandigheden die worden opgemerkt of geobserveerd. Mensen kunnen bijvoorbeeld als doel hebben effectief te werken, een opdracht op te leveren, etc. Daarnaast kunnen mensen meer sociale doelen hebben, zoals instemmen met vriendelijke verzoeken, erkend worden als een leuk, belangrijk of relevant persoon, etc. En mensen kunnen doelen hebben die betrekking hebben op hun cyberveiligheid, bijvoorbeeld hun thuisnetwerk te beveiligen, sterke wachtwoorden te gebruiken of niet meer op openbare WiFi netwerken inloggen.

Ondanks doelen die betrekking hebben op hun cyberveiligheid vertonen mensen soms risicovolle gedragingen. De meest relevante onveilige cybergedragingen hebben we opgesomd als risicogedragingen in Figuur 3-2. Deze gedragingen zijn gebaseerd op cybersecurity rapporten van Kaspersky[4], IBM[5], Accenture[6] en Symantec-Norton[7]. Om te begrijpen waarom mensen die gedragingen vertonen is het nodig aandacht te besteden aan andere doelen die mensen op enig moment nastreven, en hoe de verschillende gedragsdoelen tot stand komen en gedrag kunnen beïnvloeden. Risicovolle gedragingen zijn in wezen slechts symptomen van doelen en behoeftes. Een bredere analyse van de gedragsdoelen en achterliggende factoren levert handvatten om het risicovolle gedrag tegen te gaan.
De manier van informatieverwerking (automatisch, heuristisch of weloverwogen; zie Hoofdstuk 2 over het cyber security framework) is in grote mate afhankelijk van de beschikbare cognitieve capaciteit en motivatie om na te denken en bepaalt sterk welke psychologische processen meer of minder dominant zijn, welke doelen mentaal beschikbaar zijn, en hoe mensen die doelen bereiken (door middel van welke gedragingen). Bijvoorbeeld, iemand heeft als gedragsdoel zijn documenten veilig te bewaren. Echter, doordat er zelden veiligheidsincidenten zijn, raakt dat doel minder mentaal beschikbaar of prominent aanwezig in iemands gedachten. Daarentegen zijn tijdens interacties met anderen sociale doelen vaak juist sterker actief en hebben die een sterkere invloed op gedrag dan buiten interacties met anderen. Wanneer mensen weinig cognitieve capaciteit beschikbaar hebben, of wanneer de motivatie om na te denken over veilig gedrag niet groot is, kan dit ertoe leiden dat de actieve sociale doelen spontaan leiden tot instemming met een verzoek om een vertrouwelijk document te delen. Onder andere omstandigheden van cognitieve capaciteit of motivatie zouden de veiligheidsdoelen mogelijk meer aandacht hebben gekregen en hebben geleid tot een bewuste correctie van de behoefte om te voldoen aan een verzoek, en uiteindelijk dus tot een weigering van het verzoek.
Afhankelijk van de route door het informatieverwerkingsproces, spelen dus verschillende psychologische processen een rol die invloed hebben op de keuzes die mensen maken voor specifieke gedragingen waaronder risicovol cybergedrag. Processen die daarin relevant zijn, staan genoemd onder *psychologisch proces* in Figuur 3-2. Deze lijst is niet uitputtend en is samengesteld op basis van bestaande kennis en expertise, niet van een systematische analyse.

[4] https://www.kaspersky.com/blog/the-human-factor-in-it-security/
[5] https://www.ibm.com/security/data-breach/threat-intelligence
[6] https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
[7] http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx



Figuur 3-2 Taxonomie van slachtoffergedrag.

Deel 2: Activiteiten

Om de Cyber Security Assistent te ontwikkelen hebben wij twee activiteiten uitgevoerd:

1 Verkenning van design patterns als mogelijke kader voor interventies om cyberveilig gedrag te vergroten (Hoofdstuk 4).
2 Interviews met stakeholders om te achterhalen wat hun gebruiksbehoeften zijn en wat ze nodig zouden hebben om het meerwaarde in laten hebben in hun organisatie (Hoofdstuk 5).

4 Design Patterns

Design – of het nu gaat om het ontwerp van producten, diensten, interfaces of omgevingen – beïnvloedt het gedrag van gebruikers. Denk bijvoorbeeld aan prullenbakken die een scheef aflopende bovenzijde hebben om te voorkomen dat mensen troep bovenop de prullenbakken zetten. Medewerkers van bedrijven/organisaties gebruiken in hun dagelijkse werk allerlei computer-programma's en applicaties om hun werkzaamheden uit te voeren. Het design van deze applicaties beïnvloedt dus ook het gedrag van medewerkers, en daarmee hun cyberveilig gedrag. Het is daarom belangrijk om bij het ontwerp van applicaties, of functionaliteit binnen deze applicaties, aandacht te besteden aan het ontwerp: Hoe kunnen deze zo worden vorm gegeven dat gebruikers cyberveilig gedrag vertonen? Hier bieden design patterns mogelijk een handig hulpmiddel.
Dit hoofdstuk beschrijft design patterns: Wat zijn design patterns? Hoe kunnen design patterns worden toegepast? En hoe kunnen design patterns toegepast worden in ons werk naar interventies om cyberveilig gedrag te vergroten?

4.1 Design beïnvloedt (cyberveilig) gedrag

Elk design beïnvloedt het gedrag van gebruikers. Designers zijn zich hier echter niet altijd van bewust. Denk bijvoorbeeld aan de kleur van instrumenten in auto's. Als deze door de designer verkeerd gekozen is hebben je ogen 's nachts meer moeite om te schakelen tussen kijken naar buiten en kijken naar je instrumenten, waardoor de kwaliteit en veiligheid van het rijgedrag verminderd.
Het bewust omgaan met design kan ook helpen om allerlei sociaal maatschappelijke vraagstukken te adresseren. Lockton (2012) noemt dit 'Design with intent': "design that's intended to influence or result in certain user behaviour". Eén van deze maatschappelijke vraagstukken is cybersecurity. Dit vereist samenwerking tussen verschillende disciplines bij het ontwerpen van software applicaties. Nu zijn bij het ontwerp vaak zowel user experience (UX) designers als security consultants betrokken. Zij werken echter doorgaans niet met elkaar samen. Eén van de gevaren hiervan is dat de user experience van een product goed is maar dat de veiligheid niet op orde is of anders om.
Een oplossing hiervoor is het laten samenwerken van het UX team, het security team en de eindgebruikers. Wanneer dit vroeg in het ontwikkelproces gebeurt, kunnen security en bruikbaarheid in het product worden ingebouwd, in plaats van later een maatregel toe te voegen, zoals het vragen van een lang wachtwoord aan gebruikers. Om 'usable security' te realiseren is het belangrijk dat alle stakeholders naar elkaar luisteren: de gebruikers moeten de ontwerpers en hun ontwerpen omarmen, en de gebruikers die dagelijks met de technologie zullen moeten werken moeten door de ontwerpen optimaal worden ondersteund bij het veilig doen van hun werk.

4.2 Design patterns: een praktisch hulpmiddel

Zoals net geschetst, is het van belang om applicaties zo te ontwerpen dat ze leiden tot cyberveilig gedrag van hun gebruikers. De vraag is nu hoe je dit kunt doen.
Bij het ontwerpen van user interfaces wordt er al jaren gebruik gemaakt van richtlijnen; richtlijnen die kennis bevatten en die designers helpen bij het maken van design keuzes en die voorkomen dat telkens dezelfde ontwerpfouten worden gemaakt. Van Welie et al. (2001) geven aan dat er een aantal nadelen zit aan het

gebruik van richtlijnen. Zo zijn er veel richtlijnen en kan het lastig zijn om die richtlijnen te selecteren die van toepassing zijn op een specifiek ontwerpprobleem. Ook kunnen richtlijnen elkaar tegenspreken. En de validiteit van de richtlijnen is altijd afhankelijk van de context.
Van Welie et al. (2001) stellen daarom voor om gebruik te maken van patronen, oftewel ‘patterns’. Patterns richten zich expliciet op de context en geven aan wanneer, hoe en waarom de oplossing kan worden toegepast. De term 'design pattern' is geïntroduceerd door Christopher Alexander. Hij beschreef in zijn boek *A Pattern Language: Towns, Buildings, Construction* (1977) een ontwerpmethode voor architecten en stedenbouwkundigen. Later werd het concept design patterns ook gebruikt in software ontwikkeling en in user interface design. Een design pattern “is supposed to capture *proven* design knowledge and is described in terms of a problem, context and solution” (van Welie et al., 2001). Een pattern bestaat vaak uit meerdere geïntegreerde richtlijnen. User interface design patterns zijn beschrijvingen van ‘best practices’ binnen user interface design (Interaction Design Foundation, UI-patterns.com). Het zijn algemene, herbruikbare oplossingen voor vaker voorkomende design problemen. Designers moeten ze aanpassen voor de specifieke gebruikscontext in design projecten (Interaction Design Foundation, UI-patterns.com). Design patterns kunnen worden gebruikt als een taal tussen designers, waarbij ze met de naam van het pattern kunnen refereren aan een uitgebreide design oplossing.

4.3 De opbouw van een design pattern

Een user interface design pattern bestaat uit een aantal elementen, waarvan de context een erg belangrijke is, zoals eerder geschetst. De onderstaande tabel (Tabel 4-1) geeft een (niet uitputtend) overzicht van elementen waaruit een pattern bestaat aan de hand van een aantal bronnen.

Tabel 4-1 Onderdelen van een pattern.

Onderdeel	Toelichting	Bronnen
Naam	Naam van het pattern.	Van Welie et al. (2001), Interaction Design Foundation, Lockton (2012)
Probleem	Het usabilityprobleem dat de gebruiker ervaart bij gebruik van het systeem	Van Welie et al. (2001) , Interaction Design Foundation
Gebruikscontext	De situatie (taken, gebruikers, gebruikscontext) waardoor het usabilityprobleem ontstaat.	Van Welie et al. (2001), Interaction Design Foundation
Principe	Een pattern is doorgaans gebaseerd op één of meer design principes, zoals ‘error management’ of consistentie van user guidance.	Van Welie et al. (2001), Interaction Design Foundation, Lockton (2012)
Oplossing	Een bewezen oplossing voor het probleem. Een oplossing beschrijft alleen de kern van het probleem. De designer heeft de vrijheid om het te implementeren op veel verschillende manieren.	Van Welie et al. (2001), Interaction Design Foundation
Waarom/rationale	Hoe en waarom het pattern werkt.	Van Welie et al. (2001), Interaction Design Foundation

Onderdeel	Toelichting	Bronnen
Voorbeelden	Ieder voorbeeld laat zien hoe het pattern succesvol is toegepast in een echt systeem. Hierbij wordt er vaak een screen shot getoond en een korte beschrijving.	Van Welie et al. (2001), Interaction Design Foundation, Lockton (201)
Usability impact	Impact van het pattern op de usability.	Van Welie et al. (2001)
Implementatie	Sommige patterns bevatten ook implementatie details.	Interaction Design Foundation

4.4 Indelingen van design patterns

Patterns kunnen op verschillende manieren worden ingedeeld. Lockton (2012) deelt design patterns in acht categorieën; zogeheten 'lenzen'. Deze lenzen vertegenwoordigen verschillende 'disciplinary worldviews' of onderzoeksvelden. Voorbeelden van deze lenzen zijn de 'architectuurlens' en de 'ludieke lens'. De architectuurlens bevat technieken in het omgevingsdesign die worden gebruikt om gebruikersgedrag te beïnvloeden in architectuur, 'urban planning', verkeersmanagement en preventie van criminaliteit. Denk hierbij aan goede straatverlichting om criminelen af te schrikken de veiligheidsperceptie van de omgeving te verhogen. De ludieke lens bevat technieken om gebruiksgedrag te beïnvloeden die zijn afgeleid van games en andere speelse interacties. Er wordt gebruik gemaakt van mechanismen uit de sociale psychologie: van het stellen van doelen tot en met operante conditionering. Voorbeeld hiervan is het gebruik van 'pianotreden' om meer mensen de trap te laten nemen in plaats van de roltrap (https://www.youtube.com/watch?v=2lXh2n0aPyw)..
UI-patterns (http://ui-patterns.com/) gebruiken onder meer de categorieën 'dealing with data' en 'social'. Deze laatste categorie bevat patterns waarmee de gebruiker in staat wordt gesteld zich te verbinden, communiceren en interacteren met andere online gebruikers met als doel de gebruiker bepaald gedrag te laten tonen.
Een specifieke categorie zijn de patterns die een designer laten zien hoe h/zij kan overtuigen om bepaalde acties te doen. Deze worden ook wel 'persuasive design patterns' of 'dark patterns' (Interaction Design Foundation, http://ui-patterns.com/) genoemd. Deze laatste benaming wordt gebruikt omdat deze patterns worden ingezet in e-commerce toepassingen om gebruikers meer geld te laten besteden of persoonlijke informatie te laten bieden.
Verschillende sites bieden bibliotheken van patterns aan. Een voorbeeld is Pattern Tap (http://patterntap.com/library) .

4.5 Gebruik van design patterns in dit onderzoek

Design patterns zijn dus ontwerp- en oplossingsprincipes. Voorgenomen was om design patterns te gebruiken in dit project op twee manieren. Ten eerste, als basis voor het identificeren van oplossingsrichtingen voor cyberonveilig gedrag en om herbruikbare oplossingen in de CSA op te nemen. Hiertoe is een database ontwikkeld, waarin 247 design patterns zijn opgenomen (Bijlage B; Lockton, 2010; UI-patterns.com). Vervolgens is gepoogd principes vanuit de design patterns te vertalen naar concrete interventies die de gebruiker van de CSA handvatten geven om met het verbeteren van cyberonveilige gedrag daadwerkelijk aan de slag te gaan. In de analyse van de design patterns zijn wij echter tot de conclusie gekomen dat de meeste design patterns die bij cyberveilig gedrag van toepassing waren, zich richtten op het inhiberen of bemoeilijken van gedrag in plaats van op het faciliteren

ervan. In onze aanpak, leggen wij expliciet de nadruk op het mogelijk maken van cyberveilig gedrag in plaats van het verbieden of onmogelijk maken van cyber*on*veilig gedrag. Wij concludeerden dat er minimale variatie was in de design patterns die relevant waren voor cyberveilig gedrag, en om deze reden dus uiteindelijk ook onvoldoende aansluiting met het concept design patterns om er in het onderzoek mee verder te gaan.
Ten tweede is voorgenomen design patterns in de CSA op te nemen om de presentatie van de interventies te kunnen ordenen in categorieën gebaseerd op patterns. Dit is met name zinvol wanneer er sprake is van veel interventies per risicogedraging, waarbij een onderverdeling de begrijpelijkheid en overzichtelijkheid bevordert. Omdat bleek dat het aantal concrete interventies per gedraging beperkt was en een verdere onderverdeling overbodig zou zijn om overzichtelijkheid te bevorderen, is hier uiteindelijk van afgezien. Voor de CSA is besloten alleen interventies zelf – en niet overkoepelende patterns – op te nemen. Mocht echter in de toekomst het aantal geïdentificeerde interventies toenemen, blijft het mogelijk om design patterns alsnog op te nemen als middel om de informatie duidelijk te structureren.

5 Interviews

In het kader van de ontwikkeling van de CSA is nadrukkelijk gekeken naar de behoeftes en verwachtingen van potentiële gebruikers. Hiertoe zijn interviews gevoerd met cyber security deskundigen van verschillende grote Nederlandse bedrijven. Deze bedrijven zijn aangesloten bij de klankbordgroep van dit project. Het doel van deze interviews was het concept van de CSA te toetsen bij toekomstige gebruikers en inzicht te krijgen in wat hen vooral aansprak en welke toegevoegde waarde ze zagen in het gebruik van de CSA; danwel wat ze niet aansprak of wat ze niet als toegevoegde waarde zagen. De resultaten van deze interviews worden meegenomen in de ontwikkeling van de CSA.
In totaal zijn vijf interviews gehouden met medewerkers verantwoordelijk voor het opstellen en uitzetten van het cyber security beleid binnen hun organisatie.
Dit waren alle bedrijven die in 2017 ook betrokken waren bij het TNO onderzoek over cyberveilig gedrag, en hadden aangegeven graag betrokken te willen blijven als klankbord. Na een korte toelichting op het concept van de CSA stond een zestal vragen centraal in de gesprekken. De resultaten van de interviews zullen hieronder aan de hand van deze vragen samengevat worden.

5.1 Wat vind je van het conceptuele idee van de CSA?

De geïnterviewden vonden de CSA interessant, het idee sprak hen erg aan. Binnen het bedrijfsleven wordt gaandeweg steeds duidelijker dat awareness training niet de oplossing is voor het behalen van een bepaald veiligheidsniveau in de organisatie. Er wordt nu ook echt gezocht naar een gedragsverandering, maar het bedrijfsleven is zoekende hoe dit te bewerkstelligen. Hierbij kan de CSA ondersteunen. Ook de ‘van kop tot staart’ oplossing, oftewel de ondersteuning tot en met het meten van de effecten spreekt aan. Dit maakt het mogelijk de verandering meetbaar en daarmee zichtbaar te maken. In de dagelijkse praktijk blijkt dat binnen de organisaties, het sturen op resultaat belangrijk is om de toegevoegde waarde van een programma aan te kunnen tonen. De geïnterviewden gaven aan dat ondersteuning op dit vlak zeer welkom is.

5.2 Wie zou je de CSA laten gebruiken?

Toepassingsmogelijkheden van de CSA worden vooral gezien bij de afdelingen die zich bezig houden met het managen van de cyber security risico’s. Dit zijn afdelingen die het beleid uitzetten voor andere groepen binnen de organisatie en nadenken over maatregelen, cursussen en toepassingen om het vastgestelde beleid uit te voeren. Binnen de meeste organisaties is dit een redelijk klein team met een breed verspreidingsgebied naar de rest van de organisatie.
Daarnaast worden er ook mogelijkheden gezien voor gebruik door de lokale security en risk experts in de verschillende organisatieonderdelen. Dit betreft; een wat grotere groep. Hun taak is het implementeren van interventies binnen hun organisatie onderdelen om hiermee het beleid vorm te geven.

5.3 Stel dat jij de CSA gebruikt, hoe zou je hem gebruiken?

Uit de interviews kwam een aantal voordelen van het gebruik van de CSA naar voren:

- De CSA kan de geïnterviewden helpen zich te verantwoorden naar het hoger management. De CSA maakt duidelijk waarom bepaalde interventies nodig zijn en wat de verwachte opbrengst is. Dit helpt bij het verwerven van de budgetten die voor de interventies nodig zijn.
- Meerwaarde wordt gezien in het ondersteunen tijdens de analysefase waarin goed geduid kan worden wat er speelt en waarom bepaald gedrag vertoond wordt.
- De CSA wordt als mogelijkheid gezien om meer variatie te stimuleren binnen de bedrijfsonderdelen in de manieren waarop cyber security risico's onder de aandacht gebracht worden. Met name vind men het interessant dat deze variatie op een zodanige manier wordt vormgegeven dat het vanuit de verantwoordelijke groep eenduidig gecommuniceerd kan worden naar de rest van de organisatie en er hierdoor herhaalbare oplossingen en standaardisatie in de uitrol van oplossingen binnen de organisatie bereikt kan worden.
- De CSA helpt om de verschillende doelgroepen die binnen de grote organisaties aanwezig zijn meer op maat te kunnen bedienen.
- De volledige aanpak van analyse tot en met advisering in het meten van de effecten van maatregelen spreekt erg aan. Dit maakt het mogelijk de verandering meetbaar en zichtbaar te maken.

5.4 Hoe zou je de CSA toe willen passen binnen jouw organisatie en jouw werk?

De CSA wordt vooral gezien als ondersteuningsmiddel voor degenen die verantwoordelijk zijn voor het verbeteren van de cyber security binnen de organisatie. De tool kan hen helpen tijdens het analyseproces, inspireren bij het uitwerken van interventies en dienen als richtinggevend instrument naar anderen binnen de organisatie. Om de CSA op deze manieren te gebruiken, zijn een aantal randvoorwaarden benoemd. Dit zijn:

- De tool moet makkelijk doorzoekbaar zijn, omdat er uiteindelijk veel gedragingen in opgenomen zullen worden;
- De tool moet kunnen bijhouden wat je gedaan hebt en welke ervaringen daarmee opgedaan zijn: wat werkt wel en wat werkt niet;
- De tool moet aangepast kunnen worden naar de eigen organisatie; inhoudelijk gevuld worden voor de eigen organisatie;
- De tool moet een palet aan interventies bieden, gekoppeld aan bepaalde situaties of doelgroepen;
- Er moet in de tool met verschillende rechten voor verschillende soorten gebruikers gewerkt kunnen worden.
  - Administratorrechten voor de mensen die verantwoordelijk zijn voor het uitzetten van het beleid en hiervoor analyses doen, een palet aan interventies selecteren, verantwoordelijk zijn voor het meten, etc.
    Zij bereiden de CSA als het ware inhoudelijk voor, voor het gebruik binnen de rest in de organisatie.
  - Gebruikersrechten voor verantwoordelijken binnen de andere groepen die uit de mogelijke interventies iets kiezen om binnen hun eigen onderdeel uit te rollen.

Ook werd een aantal behoeften genoemd, waarbij de CSA zou kunnen ondersteunen:

- Hulpmiddel bieden voor het vaststellen van het gedrag van de medewerkers. Bijvoorbeeld handvatten voor het uitvragen van achterliggende gedragingen.
- Het opnemen van verschillende doelgroepen in de tool, wat zijn kenmerken van verschillende doelgroepen en hebben deze misschien verschillende aanpakken nodig.
- Ondersteuning bieden bij het prioriteren van onderwerpen die aangepakt kunnen worden.
- Mogelijkheid advies te vragen aan TNO.
- Resultaten visueel aantrekkelijk weergeven zodat senior management makkelijk overtuigd kan worden.

De CSA wordt ook gezien als een tool die een ‘cyber security’ community kan ondersteunen, over bedrijven heen. Binnen deze community wil men verschillende interventies en de ervaringen daarmee met elkaar delen. De komende jaren is de verwachting dat door schaarste op de arbeidsmarkt het community aspect steeds belangrijker zal worden, er zijn te weinig mensen in Nederland die dit werk kunnen doen en je elkaars personeel niet wilt wegstelen. Informatie delen binnen een community houdt natuurlijk wel wat veiligheidsaspecten in, zo zal niet alle informatie breed gedeeld kunnen worden. Een beveiligde laag binnen de eigen organisatie zou gewenst zijn, waar eigen risico’s en interventies vastgelegd en gedeeld worden.

5.5 Zie je ook nadelen of risico’s aan het gebruik?

Als mogelijke nadelen werden genoemd dat men de CSA teveel zou volgen; dat men zelf niet meer nadenkt; dat men de input altijd accepteert en van de aangeboden oplossingsrichtingen niet meer kritisch kijkt of ze wel bij de organisatie passen; of dat men niet verder kijkt dan de oplossingsrichtingen die door de CSA geboden worden. De CSA wordt als ondersteunings- en inspiratiemiddel gezien. Het is voor de geïnterviewden erg belangrijk dat de gebruikers zelf kritisch blijven nadenken en de vertaalslag naar hun eigen organisatie maken.

5.6 Stel dat de CSA alles zou kunnen doen wat jij zou willen, wat zou hij dan absoluut (regelmatig) voor jou doen?

Op deze vraag werden de volgende antwoorden gegeven:

- Management overtuigen waarom een interventie die geld kost toch de beste optie is en gekozen moet worden;
- Palet aan interventies geven gekoppeld aan bepaalde situaties;
- Tailoren/aanpassen naar de eigen organisatie;
- Output: KPI’s en effectmetingen;
- Resultaten in de tool kunnen zien: dashboard waarop je kunt sturen. Welke acties zijn gedaan, waarop is gezocht, index, wat heeft een interventie opgeleverd?
- Hulp bieden bij het verzamelen van waarheid gebonden input van medewerkers;
- Focussen op doelgroepen en hier de output op baseren;
- Ondersteuning bij het prioriteren van onderwerpen.

Deel 3: Tools, Ondersteuning en Evaluatie

De uitkomsten van dit onderzoek zijn:

1 Het belangrijkste resultaat van dit onderzoek is de Cyber Security Assistent (CSA). Dit is een tool waarmee mensen die verantwoordelijk zijn voor de cyberveiligheid van hun organisatie ondersteund kunnen worden in dat proces (Hoofdstuk 6).
2 Om cyberveiligheid succesvol te managen, is inzicht in het niveau van cyberveiligheid alsook in de effecten van je interventies essentieel. Wij beschrijven hoe dit gedaan kan worden (Hoofdstuk 7).
3 De CSA en inzichten in het meten van cyberveiligheid zijn samen met stakeholders geëvalueerd in de Workshop Veilig Werken (Hoofdstuk 8).

6 Cyber Security Assistant

Om de inhoudelijke inzichten beschreven in Hoofdstukken 2 en 3 te ontsluiten naar organisaties en de mensen die daarin verantwoordelijk zijn voor cybersecurity, ontwikkelden wij in 2018 de Cyber Security Assistent (CSA). In dit hoofdstuk beschrijven wij wat de Cyber Security Assistent is, de beoogde gebruikersgroepen en hoe en waarvoor de CSA gebruikt kan worden. Het concept van de CSA is op verschillende wijzen getoetst met gebruikers: interviews, Workshop Veilig Werken (met onder andere de vragenlijst Cyberproblematieken) en een veldtest met een groot Nederlands particulier bedrijf. De interviews, de workshop en de vragenlijst worden in respectievelijk Hoofdstukken 5, 8.1 en 8.2 gerapporteerd. De veldtest vindt plaats in de tweede helft van 2018 en zal in het tweede rapport van dit project beschreven worden.
De CSA is een digitale tool die op een gestructureerde manier ondersteunt bij de gedragsanalyse van cyber onveilig gedrag. Vervolgens helpt de CSA het gedrag te koppelen aan passende en concrete cybersecurity oplossingen oftewel interventies te komen.
De CSA is bedoeld voor mensen die de taak hebben cybersecurity binnen bedrijven te vergoten, handhaven en monitoren, en die geen achtergrond hebben in de sociale wetenschappen. Mogelijke gebruikers zijn:

- Cybersecurity experts binnen de security afdeling van grote organisaties.
- Ondernemers van kleinere bedrijven die geen dedicated security afdeling of experts hebben en hun cybersecurity willen vergroten.
- Consultants die securitydiensten aanbieden aan klanten, en hun dienstenportfolio willen verbreden.

De CSA kan gewoon op de werkplek of een mobiel device gebruikt worden. Door middel van een aantal stappen waar keuzen gemaakt kunnen worden, wordt de gebruiker door het gedragsanalyseproces geloodst. De CSA bevat:

- Ondersteuning bij de probleemanalyse (welke kwetsbaarheden zijn er, welk probleemgedrag speelt, welke risico's horen hierbij er en welke verklarende factoren voor dat probleemgedrag zijn er).
- Handvatten en concrete suggesties voor passende interventies. Vervolgens is het aan de gebruiker daadwerkelijk interventies te implementeren binnen de organisatie.
- Tips voor het meten van de effecten van interventies.

Om een idee te geven van hoe een CSA er uit kan zien, is een prototype ontwikkeld waarin drie cyber onveilige gedragingen zijn uitgewerkt. Dit prototype geeft een overzicht van te doorlopen stappen om het daadwerkelijke probleem te analyseren en te komen tot mogelijke interventies. De cyber onveilige gedragingen die zijn uitgewerkt, zijn:

- Gebruik van ICT middelen voor zowel werk- als privé doeleinden;
- Gebruik van onveilige netwerken;
- Klikken op onveilige links.

Input voor de CSA is verkregen uit verschillende bronnen:

- Ons werk in 2017, o.a. de ontwikkeling van de TNO Cybersecurity Framework (van Vliet et al., 2017);
- Interviews met cybersecurity professionals in 2018 (zie Hoofdstuk 5);
- Een vragenlijst uitgezet tijdens de Workshop Veilig Werken in juni 2018 (zie Hoofdstuk 8.2);
- Analyse van psychologische antecedenten gerelateerd aan cyberonveilig gedrag (zie Hoofdstuk 3);
- Sessies met psychologische domeinexperts om achterliggende motieven en doelen te identificeren van medewerkers die cyberonveilig gedrag vertonen.

In de volgende paragrafen illustreren we het CSA prototype aan de hand van het cyberonveilige gedrag: ‘Gebruik van onveilige netwerken’. Het is goed om te realiseren dat de CSA in dit stadium alleen nog gebruikt wordt voor workshops met experts die met deze methode aan de slag gaan en input geven over het mogelijke gebruik van de CSA. Hierbij wordt de CSA als middel gebruikt om te discussiëren over cyberproblematiek binnen organisaties en op welke manier de CSA hierbij zou kunnen ondersteunen.

6.1 Het CSA prototype

6.1.1 Begin scherm CSA: Stap 1: Van welk cyberonveilig gedrag is er sprake?

In de eerste stap vraagt de CSA de gebruiker om te kiezen van welk cyberonveilig gedrag er sprake is. In het prototype zijn de gedragingen die verder uitgewerkt zijn in de CSA zwart gedrukt. De gedragingen die als relevant zijn benoemd door experts, maar niet zijn uitgewerkt, verschijnen in het grijs. Aan de rechter kant van het begin scherm staat extra toelichting.

Figuur 6-1 Begin scherm CSA: Stap 1: Van welk cyberonveilig gedrag is er sprake?

Als de gebruiker klikt op ‘meer weten?’, popt er een scherm met aanvullende informatie op. In dit scherm wordt aanvullende informatie gegeven over de CSA. Mocht in een vervolgstadium de CSA breder worden uitgezet, dan dient deze informatie als standaard startscherm gepresenteerd te worden om de gebruiker nadere informatie te bieden over het gebruik van de CSA. Hieronder is deze aanvullende informatie beschreven:

Wat is de Cyber Security Assistent?
De Cyber Security Assistent (CSA) helpt cybersecurity medewerkers te bepalen hoe binnen hun organisatie veilig cybergedrag gefaciliteerd kan worden. Door middel van het doorlopen van een gestructureerd proces wordt inzicht verkregen in welke gedragsfactoren van de cybersecurity verbeterd kunnen worden. De CSA bevat:
1) Ondersteuning bij de probleemanalyse: welke kwetsbaarheden zijn er, welk problematisch gedrag speelt er en welke verklarende factoren zijn er voor dat gedrag?
2) Handvatten en concrete suggesties voor het vormgeven van passende interventies.
3) Tips voor de effectmeting van resultaten van interventies.

Waarom de Cyber Security Assistent?
Hoe goed IT-systemen technisch ook beveiligd zijn, incidenten zijn niet uit te sluiten. Ten eerste omdat criminelen, hackers en dergelijke zullen blijven zoeken naar gaten in de beveiliging. Ten tweede omdat cybercriminelen juist door toegenomen technische beveiliging van ICT hun aandacht lijken te verleggen naar de kwetsbaarheid van de gebruikers van de systemen die ze willen compromitteren (Security.nl, 2012). Gebruikers van software maken zichzelf van tijd tot tijd kwetsbaar door onveilige sites te bezoeken, of wegen te zoeken om gemakkelijker hun doelen te bereiken, te verzuimen hun software te updaten, of zich direct of indirect te laten overreden om gevoelige informatie weg te geven. Een oorzaak hiervan lijkt te liggen in het vertrouwen dat men heeft in de veiligheid van ICT en een gebrek aan een gezond wantrouwen. Veel bedrijven wapenen zich tegen deze menselijke risico's door hun personeel via awareness programma's en trainingen bewust te maken van cyberrisico's en hoe daarmee om te gaan. Helaas laat de werkelijkheid zien dat, hoe noodzakelijk bewustwording ook is, dit in veel gevallen niet voldoende is om het gewenste effect te bereiken.
Maar hoe bereik je dan wel het gewenste effect? Hoe zorg je voor passende interventies die inspelen op de redenen die mensen hebben om cyberonveilig gedrag te vertonen? De CSA ondersteunt op een gestructureerde manier het analyse- en ontwerpproces om tot passende oplossingen te komen.

Waarom werken awareness programma's niet?
In de praktijk zijn bewustwordingsprogramma's voor cybersecurity niet altijd effectief. Dit komt onder andere doordat risicovol gedrag wordt verboden in plaats van te zoeken naar alternatieven waarmee medewerkers hun doelen op een cyberveilige manier kunnen bereiken. Veilig cybergedrag ontstaat niet door het veranderen van gedrag, maar door het faciliteren van dat gedrag op een veilige manier.

Voor wie is de Cyber Security Assistent?
De Cyber Security Assistent is bedoeld voor diegenen die binnen hun organisatie aangewezen zijn voor het verbeteren van de cybersecurity.

Hoe gebruik je de Cyber Security Assistent?
De Cyber Security Assistent is een online tool. In drie stappen wordt de cybersecurity specialist door het gedragsanalyseproces geleid. Op basis van de keuzes worden suggesties gedaan voor het verhogen van cyberveilig gedrag. De cybersecurity specialist kan de interventies implementeren binnen de organisatie. De Cyber Security Assistent geeft tevens suggesties over de inrichting van effectmetingen.

Vragen of opmerkingen?
Wilt u meer weten over de Cyber Security Assistent of over het onderzoek dat we doen? Neem dan contact op met: Dr Heather Young. Per email: heather.young@tno.nl, of telefonisch: +31 88 866 59 31 / +31 6 2246 1065.

6.1.2 Stap 2: Definiëren van het cyberonveilige gedrag

De gebruiker kan vervolgens een cyberonveilig gedrag aanklikken om naar het volgende scherm te gaan. In dit voorbeeld is er op het gedrag ‘gebruik van onveilige netwerken’ geklikt. Aan de rechter kant van het scherm vindt de gebruiker een toelichting van de risico’s van het gedrag. Maar hij/zij kan ook klikken op de blauw gekleurde link: ‘klik hier voor meer toelichting over hoe gedrag tot stand komt’. Als de gebruiker op deze link klinkt dan verschijnt de volgende informatie:

Figuur 6-2 Stap 2: Definiëren van het cyberonveilige gedrag.

Hoe zorg je dat medewerkers cyberveilig werken?
Er wordt geschat dat mogelijk 95% van alle cyberincidenten te wijten is aan menselijk handelen. Cyberincidenten zijn daarmee veel meer een menselijk probleem dan een technisch probleem. Mensen bewust maken van de risico's is niet voldoende om cyberincidenten te voorkomen. Sommige gedragingen, zoals klikken op links, vinden automatisch plaats, zonder dat mensen erover nadenken. In het kort zijn er drie verschillende manieren waarop gedrag tot stand komt:

Automatisch gedrag is verantwoordelijk voor het grootste deel van wat wij dagelijks doen. Denk bijvoorbeeld aan het hard op de rem trappen als je voorligger dat ook doet. In de cyber-omgeving klik je in een moment van onoplettendheid automatisch op een phishing link: link, klik, klaar!

Gewoontegedrag bestaat uit de dingen die we vaak doen en waarover we slechts een beetje hoeven na te denken. Bijvoorbeeld het kiezen van de route die je 's ochtends naar je werk neemt: makkelijk, maar net niet automatisch. Je checkt misschien de verkeersinformatie voordat je vertrekt, maar in principe neem je altijd dezelfde route ondanks dat een andere route wellicht korter of sneller zou zijn. In een cyber-omgeving kun je denken aan het gebruik van WiFi in de trein om op weg naar huis de laatste loodjes van het werk nog even af te handelen: niet veilig, wel een gewoonte.

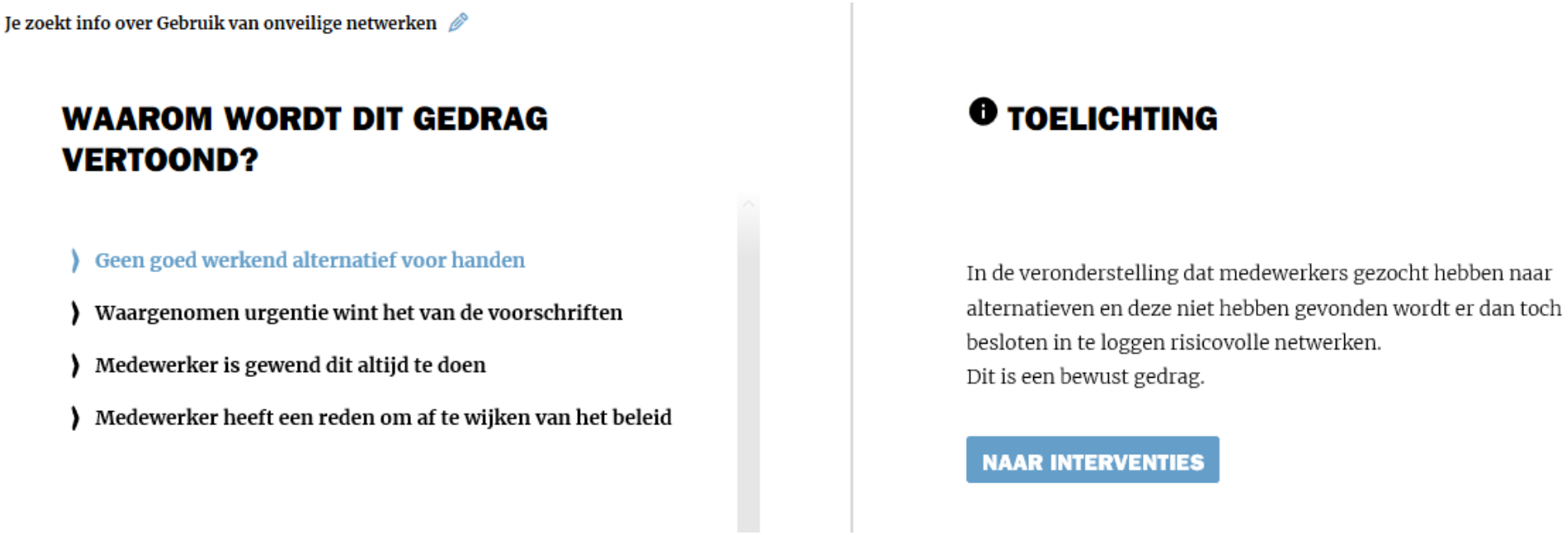
Weloverwogen gedrag is gedrag waarbij we echt moeten nadenken over iets dat we niet vaak tegenkomen. Bijvoorbeeld het afsluiten van een hypotheek. Welke vormen heb je met welke voordelen? Wat is het beste voor mij? Kan ik beter een adviseur in de arm nemen? In de cyber-omgeving kun je denken aan inrichten van de veiligheid van je thuisnetwerk. Hier gelden dezelfde vragen als bij het afsluiten van een hypotheek. Wellicht ook met dezelfde onzekerheid over de antwoorden. Het probleem met weloverwogen gedrag is dat mensen er meestal weinig zin in hebben: het kost veel mentale energie en tenzij de motivatie en noodzaak groot genoeg zijn, zijn we eerder geneigd om ons er niet voor in te spannen. Dit is geen kwestie van luiheid, maar van beperkte mentale middelen die we gericht en geprioriteerd moeten inzetten.

6.1.3 Stap 3: Waarom wordt dit gedrag vertoond?

In de volgende stap kan de gebruiker aangeven waarom hij/zij denkt dat dit gedrag wordt vertoond. Door een goede inschatting te maken van waarom medewerkers het gedrag vertonen, kunnen passende interventies ingezet worden. In dit voorbeeld heeft de gebruiker vier opties. In deze rapportage werken we alle vier de opties uit.

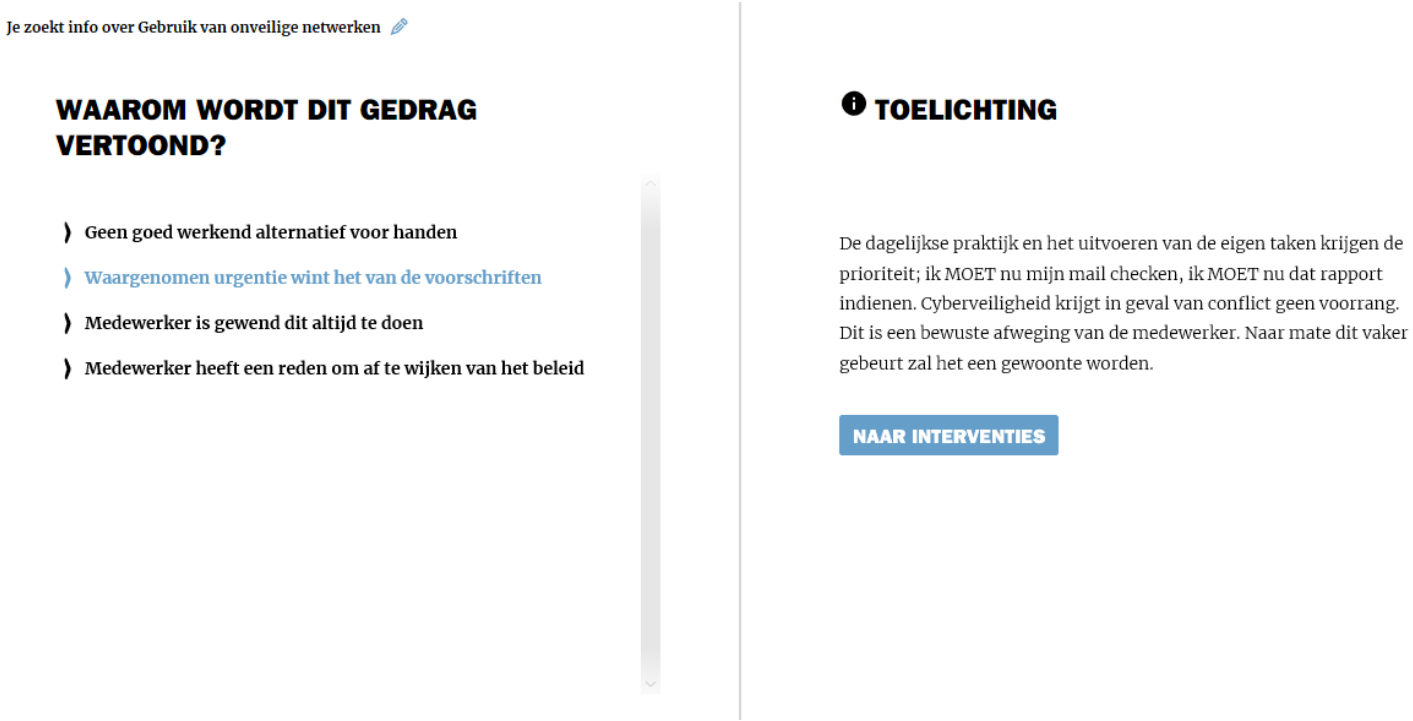
Figuur 6-3 Stap 3: Waarom wordt dit gedrag vertoond?

Als de gebruiker de eerste optie aanklikt: ‘geen goed werkend alternatief voor handen’ krijgt de gebruiker de volgende toelichting (Figuur 6-4, rechter kant van het scherm).



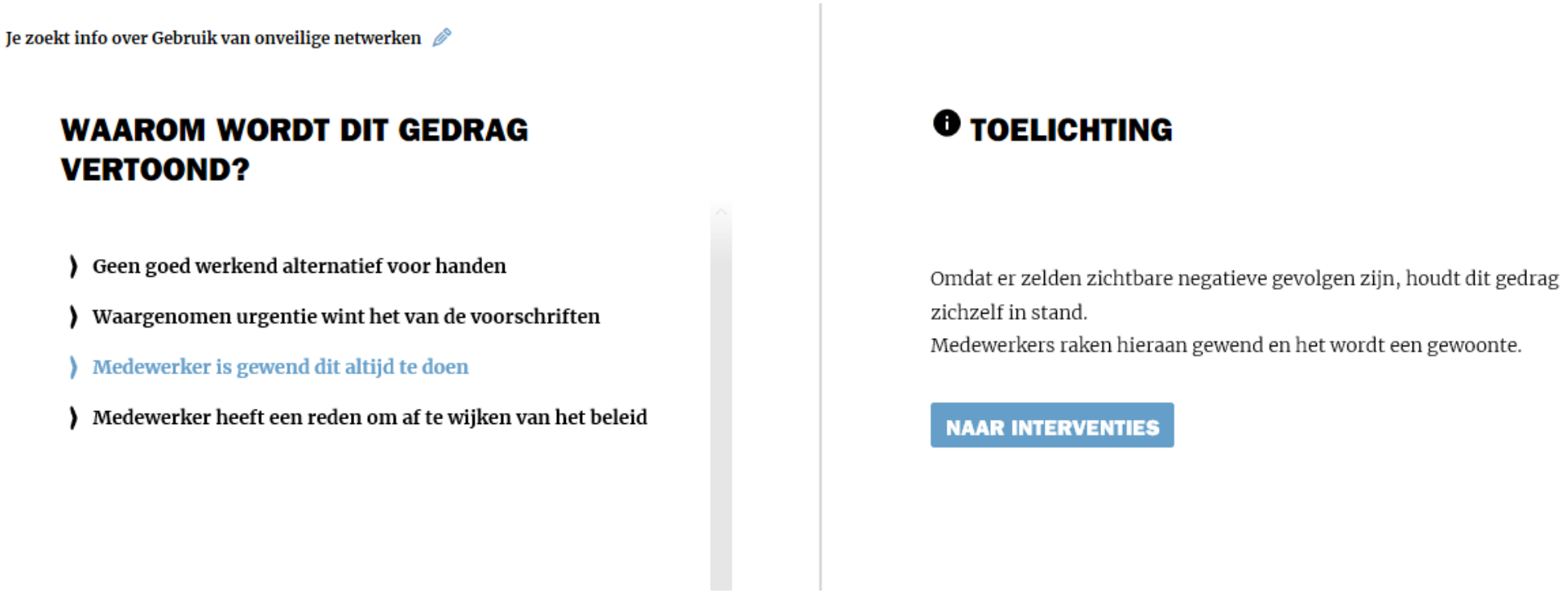
Figuur 6-4 Stap 3: Waarom wordt dit gedrag vertoond? Geen goed werkend alternatief voor handen.

Als de gebruiker de tweede optie aanklikt: ‘waargenomen urgentie wint het van de voorschriften’ dan krijgt de gebruiker de volgende toelichting (Figuur 6-5, rechter kant van het scherm).



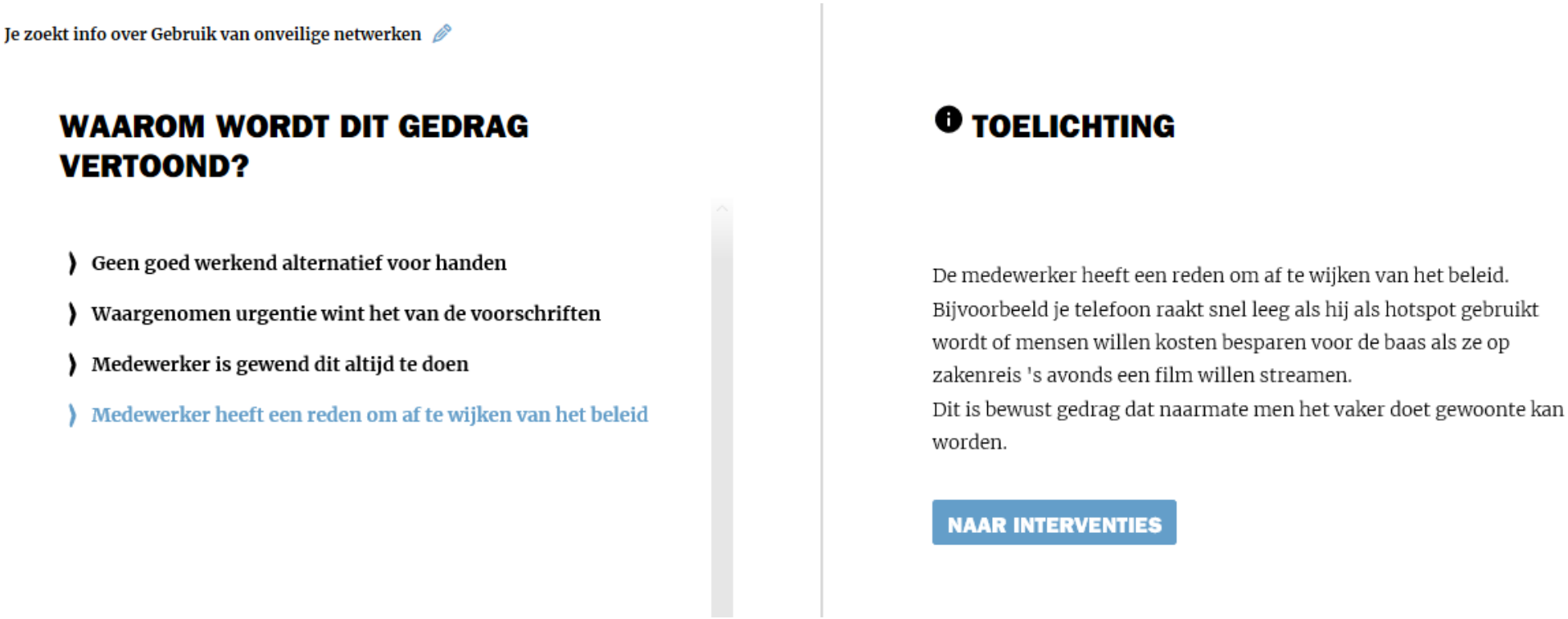
Figuur 6-5 Stap 3: Waarom wordt dit gedrag vertoond? Waargenomen urgentie wint het van de voorschriften.

Als de gebruiker de derde optie aanklikt: ‘medewerker is gewend dit altijd te doen’ dan krijgt de gebruiker de volgende toelichting (Figuur 6-6, rechter kant van het scherm).



Figuur 6-6 Stap 3: Waarom wordt dit gedrag vertoond? Medewerker is gewend dit altijd te doen.

Als de gebruiker de vierde optie aanklikt: ‘Medewerker heeft een reden om af te wijken van het beleid’ dan krijgt de gebruiker de volgende toelichting (Figuur 6-7, rechter kant van het scherm).



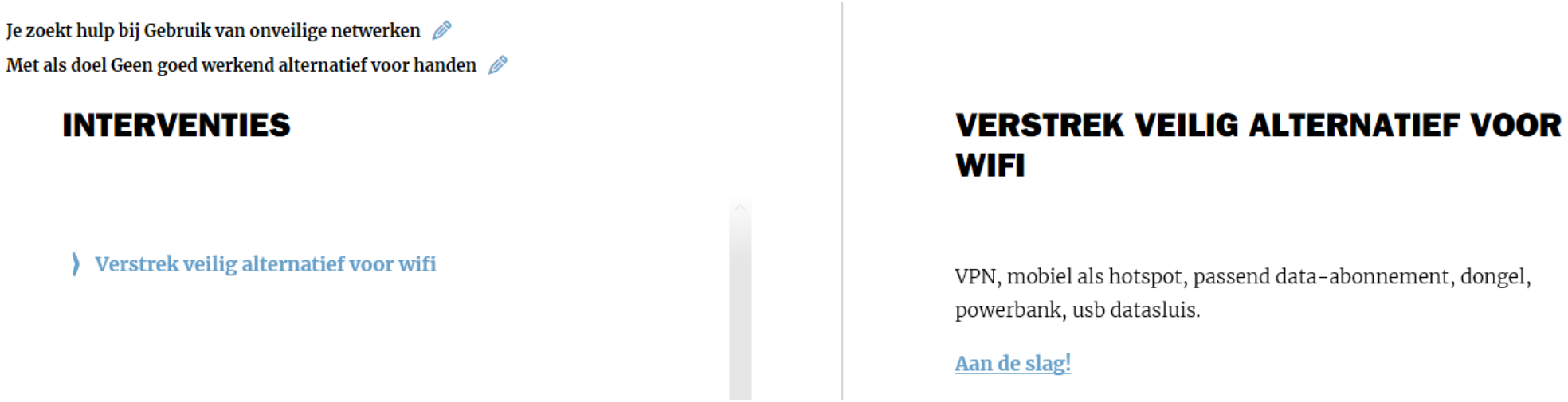
Figuur 6-7 Stap 3: Waarom wordt dit gedrag vertoond? Medewerker heeft een reden om af te wijken van het beleid.

6.1.4 Stap 4: Interventies

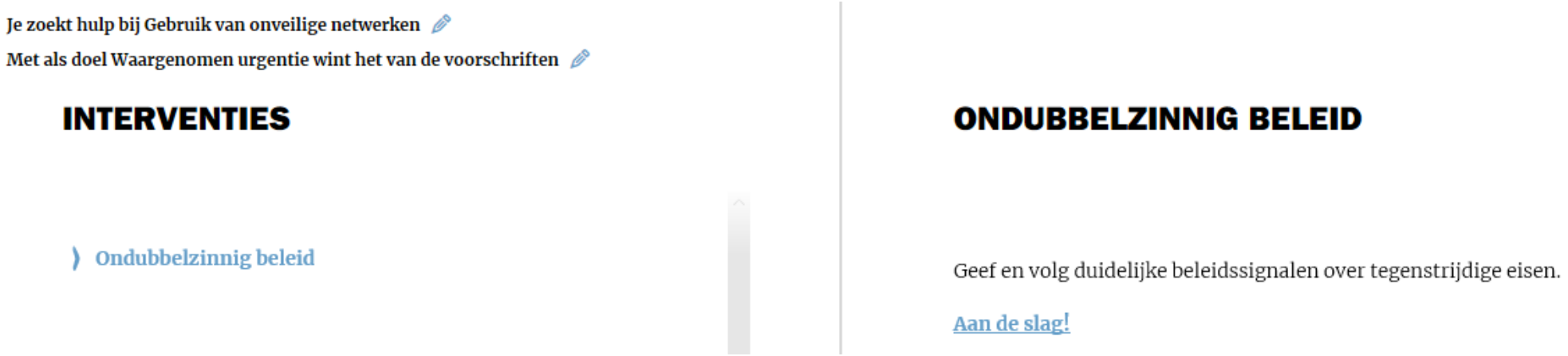
Op basis van het gekozen cyberonveilige gedrag en de reële reden voor dit gedrag, worden interventies aangedragen. Deze interventies bestaan uit een voorbeelden van typen interventies, en geven uitleg van deze concepten. Het daadwerkelijk implementeren van een interventie in een organisatie is namelijk maatwerk. Eenmaal aangekomen in het interventie deel van de CSA wordt standaard onderstaande tekst gepresenteerd.

Figuur 6-8 Interventies toelichting.

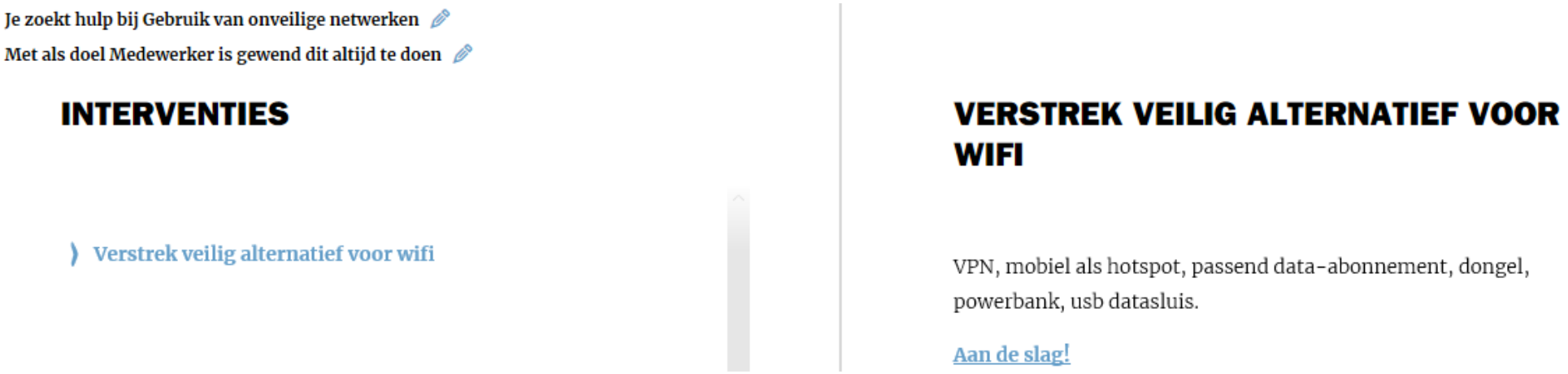
Als de gebruiker klikt op een interventies dan komt er informatie naar boven met voorbeelden van de interventie. Hieronder worden de verschillende interventies getoond, gekoppeld aan het cyber onveilige gedrag en de achterliggende doelen.



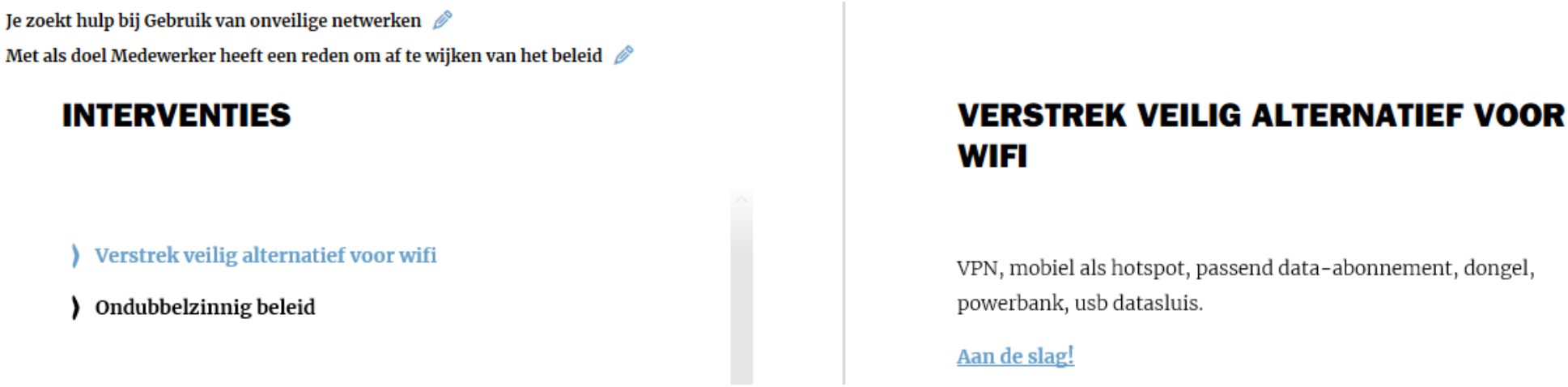
Figuur 6-9 Gebruik van onveilige netwerken. Met als doel Geen goed werkend alternatief voor handen.



Figuur 6-10 Gebruik van onveilige netwerken. Met als doel Waargenomen urgentie wint het van de voorschriften. Interventie toelichting.



Figuur 6-11 Bij Gebruik van onveilige netwerken. Met als doel Medewerker is gewend dit altijd te doen. interventie toelichting.



Figuur 6-12 Gebruik van onveilige netwerken. Met als doel Medewerker heeft een reden om af te wijken van het beleid. Interventie verstrek veilig alternatief voor wifi toelichting.

Figuur 6-13 Gebruik van onveilige netwerken. Met als doel Medewerker heeft een reden om af te wijken van het beleid. Interventie ondubbelzinnig beleid toelichting.

6.1.5 Stap 5: aan de slag!

Onder de toelichting van iedere interventie is de link ‘aan de slag’ te vinden. De informatie onder die link is in dit prototype voor iedere interventie hetzelfde. Als de gebruiker op deze link klikt, komt er informatie naar boven over de vereiste maatwerkoplossingen voor het implementeren van interventies, en krijgt de gebruiker mogelijke opties voor het evalueren van de interventies. Hier worden verschillende meetinstrumenten genoemd. Hieronder is de toelichting zoals in de CSA beschreven vinden.

Aan de slag
Op basis van deze voorbeelden kunt u uw eigen interventie ontwikkelen. Interventies zijn vaak maatwerk oplossingen voor organisaties en niet één op één te kopiëren. Echter, de onderliggende mechanismen zijn beproefde oplossingsrichtingen en kunnen als inspiratie dienen voor uw eigen oplossingen.
Hoe nu verder?
Het is belangrijk om de effecten van een interventie te kunnen evalueren. Om de meerwaarde van de interventies aan te kunnen tonen kunt u bijvoorbeeld denken aan de volgende metingen. (Let hierbij wel op dat de meting aansluit bij de interventie die u toepast.)

- Loggen aantal geüpdatete systemen
- Vragenlijstonderzoek
- Toename/afname incident-registratie
- Toename/afname gebruik vreemde/onveilige netwerken
- Toename/afname geregistreerde virussen, trojans, etc.
- Toename/afname geklikte onveilige hyperlinks/websites

Heeft u nog vragen na aanleiding van dit prototype? Neem dan gerust contact op met Dr Heather Young: **heather.young@tno.nl**.

7 Effectmetingen en KPI's

7.1 Inleiding

Beoogd onderdeel van de CSA wordt in de verder doorontwikkeling ervan informatie (bijvoorbeeld via een module) over het vaststellen en monitoren van het niveau van cyberveiligheid van een organisatie. Ook wordt informatie opgenomen over het bepalen van het effect en de effectiviteit van een interventie. In dit hoofdstuk beschrijven wij systematieken hiervoor.
Eerder hebben we vastgesteld dat de veiligheidstoestand van het cybersysteem niet alleen afhankelijk is van 'machine' gedrag maar ook afhankelijk is van (on)veilig cyber gedrag van mensen (van Vliet et al., 2017). De CSA is een hulpmiddel voor cyberspecialisten om gedragsverandering bij mensen te faciliteren. Dat kan zowel het verhinderen van onveilig gedrag als het stimuleren van veilig gedrag. Om te kunnen nagaan of ontworpen en geïmplementeerde interventies daadwerkelijk een gedragsverandering bewerkstelligd hebben, en daarmee de toestand van cyberveiligheid bevorderden, is het van het grootste belang om niet alleen het (on)gewenste gedrag van machines te monitoren zoals nu al gebruikelijk is, maar ook van de mens. Meten is weten.
Dit kan globaal op twee manieren gebeuren.

- rechtstreeks vragen aan de mensen of zij zich anders zijn gaan gedragen of de intentie hebben/hadden om zich anders te gedragen. Dit kan via interviews en/of vragenlijsten. Doorgaans geven deze een reflectie op de perceptie van een toestand uit het verleden of een perceptie van de toekomst. Let wel, vragenlijsten en/of interviews leveren vrijwel altijd percepties op; en deze hoeven niet altijd in overeenstemming te zijn met daadwerkelijk gedrag.
- door middel van (objectieve) observaties van gedrag. Dat kan op allerlei manieren plaatsvinden zoals bijvoorbeeld kijken, video- en/of spraakopnamen, en andere registratiemethoden zoals loggen van cybergedrag. Observaties registreren het 'hier en nu' gedrag en zijn daarom doorgaans betrouwbaarder als het gaat om daadwerkelijk gedrag.

Interviews en vragenlijsten hebben als nadeel dat de reguliere werkzaamheden, die via het cybersysteem plaatsvinden, worden verstoord omdat er extra handelingen moeten worden verricht door de mensen. De ervaring leert ons dat de interrupties worden door mensen als vervelend ervaren, waardoor ze geen aandacht meer besteden aan die vragenlijsten (en ze dus niet of minder goed/nauwkeurig/gedetailleerd invullen), waardoor het middel (de vragenlijst) verliest aan betrouwbaarheid en validiteit.
Observaties, en in het bijzonder het loggen van cybergedrag, hebben dit nadeel niet; de mensen worden niet in hun activiteiten gestoord. Een nadeel van deze benadering is dat, indien niet expliciet duidelijk wordt gemaakt aan mensen dat het loggen op een anonieme wijze gebeurt, met andere woorden dat het individu niet te traceren is bij de interpretatie van de gegevens, er een gevoel van onbehagen gaat prevaleren en de privacy in het geding is. Dit is geen wenselijke toestand voor een organisatie en moet worden vermeden, bovendien zijn er wettelijke richtlijnen[8] waaraan moet worden voldaan. Dit geldt overigens ook voor de vastlegging van interview- en vragenlijstgegevens.

[8] Zie: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving

7.2 Aanpak

In het rapportage van ons onderzoek in 2017 (van Vliet et al., 2017) zijn we ingegaan op een systematiek voor het genereren van Key Performance Indicators (KPI's) waarmee kan worden nagegaan:

- Hoe cyberveiligheid wordt waargenomen door de tijd;
- Hoe cyberveilig gedrag toe- of afneemt door de tijd.

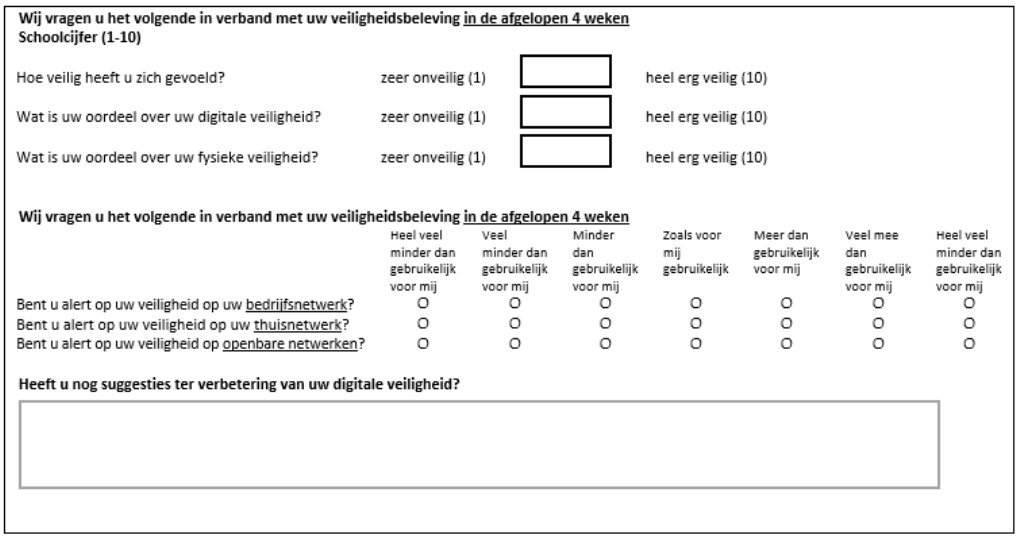
Met beide indicatoren valt dan vast te stellen of zowel de waargenomen veiligheid toe- of afneemt en de (on)veilige gedragingen toe- of afnemen. Beide inzichten zijn noodzakelijk om de effectiviteit van interventies en de veiligheid van het cybersysteem te appreciëren.

7.3 Het meten van perceptie van cyberveiligheid

Een experimentele algehele cybersecurity perceptiemonitor is ontwikkeld die de alertheid voor veiligheid meet. Dit instrument zou op herhaalde basis moeten worden afgenomen om ook de verandering in perceptie van veiligheid door de tijd te kunnen meten. Dit is van belang om de wijzigingen in perceptie te kunnen monitoren en te kunnen nagaan of interventies het gewenste effect hebben. Deze vragenlijst *perceptie van (cyber)security* bestaat uit drie onderdelen waarop respondenten gevraagd wordt hun oordeel te geven over de afgelopen vier weken:

a) Absolute oordelen over gevoel van veiligheid in het algemeen, fysiek en digitaal;
b) Relatieve oordelen over alertheid op veiligheid in drie omgevingen: op het werk, thuis en op openbare netwerken;
c) Een ruimte voor suggesties en opmerkingen.

Hieronder wordt in Figuur 7-1 deze korte vragenlijst weergegeven.



Wij vragen u het volgende in verband met uw veiligheidsbeleving in de afgelopen 4 weken
Schoolcijfer (1-10)

Hoe veilig heeft u zich gevoeld?	zeer onveilig (1)	☐	heel erg veilig (10)
Wat is uw oordeel over uw digitale veiligheid?	zeer onveilig (1)	☐	heel erg veilig (10)
Wat is uw oordeel over uw fysieke veiligheid?	zeer onveilig (1)	☐	heel erg veilig (10)

Wij vragen u het volgende in verband met uw veiligheidsbeleving in de afgelopen 4 weken

	Heel veel minder dan gebruikelijk voor mij	Veel minder dan gebruikelijk voor mij	Minder dan gebruikelijk voor mij	Zoals voor mij gebruikelijk	Meer dan gebruikelijk voor mij	Veel mee dan gebruikelijk voor mij	Heel veel minder dan gebruikelijk voor mij
Bent u alert op uw veiligheid op uw bedrijfsnetwerk?	O	O	O	O	O	O	O
Bent u alert op uw veiligheid op uw thuisnetwerk?	O	O	O	O	O	O	O
Bent u alert op uw veiligheid op openbare netwerken?	O	O	O	O	O	O	O

Heeft u nog suggesties ter verbetering van uw digitale veiligheid?

Figuur 7-1 Voorbeeld cybersecurity perceptiemonitor.

De rationale voor deze opzet wat betreft de oordelen over veiligheidsgevoel (onderdeel *a*) is erin gelegen dat we verwachten dat er een sterkere relatie gaat ontstaan tussen algehele gepercipieerde veiligheid en digitale gepercipieerde veiligheid in de komende jaren. Dit zou tot uiting moeten komen in een steeds hogere de samenhang tussen algehele gepercipieerde veiligheid en de digitale

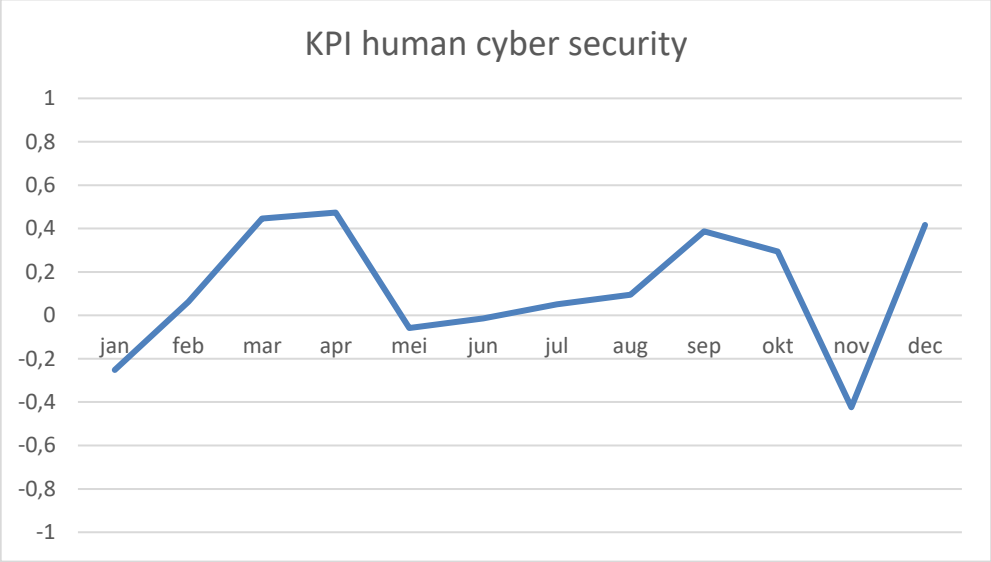
gepercipieerde veiligheid. Deze verandering(hogere samenhang) zou kunnen duiden op een toename in de ‘cybersecurity awareness’.
Het tweede onderdeel (*b*) betreft alertheid in drie omgevingen die met een relatieve 7-puntsschaal worden bevraagd. Deze constructie is met opzet relatief gekozen omdat op deze manier een grotere sensitiviteit wordt bewerkstelligd voor recente veranderingen (interventies). Immers, we gaan ervan uit dat de interventies effect zullen hebben, niet alleen op het gedrag, maar ook op de perceptie van veiligheid en alertheid.

7.4 Het meten van cyberveilig gedrag

Bij voorkeur heeft een organisatie een zeer beperkt aantal Key Performance Indicators (KPI’s) waarop de ‘performance’ van een organisatie gemonitord wordt. Voor de toestand *cybersecurity* zouden dat er twee kunnen zijn: ‘machine cybersecurity’ en ‘human cybersecurity’. Hier beperken we ons tot ‘human cybersecurity’. Een dergelijke ‘human cybersecurity KPI’ kan een samenstelling zijn van een aantal relevante gedragingen van medewerkers die de veiligheid van het cyber systeem beïnvloeden. Om tot een dergelijke KPI te komen is het van belang na te gaan welke dreigingen en reacties daarop in een bepaalde periode relevant zijn. Per periode (jaar of jaren) stelt een organisatie vast wat de belangrijkste cyber security dreigingen zijn en maakt zij een keuze voor een beperkt aantal gedragingen die in deze periode de input zijn. In het geval van cybersecurity kunnen gedragingen bijvoorbeeld zijn:

- Toename/afname in aantal keren geklikt op een link in een phishing mail tussen twee tijdsperiodes;
- Toename/afname in aantal keren dat men gemeld heeft dat men ge-phisht is tussen twee tijdsperiodes;
- Toename /afname in de lengte van wachtwoorden tussen twee periodes;
- De toename/afname in tijdsduur tussen beschikbaarheid van updates en implementatie van updates tussen twee tijdsperiodes.

Op die manier is de KPI ‘human cyber security’ een herkenbare ‘vaste’ indicator voor managers, maar met de jaren veranderen de gedragingen die als input dienen voor de KPI omdat de dreigingen ook veranderen en andere gedragingen kunnen beïnvloeden. Bovendien is van belang dat adequaat door medewerkers wordt gereageerd op dreigingen. Om dit op een effectieve manier te operationaliseren is het belangrijk na te denken hoe gedrag te veranderen. Met andere woorden, vaststellen of de gewenste veranderingen in gedrag hebben plaatsgevonden.
De ‘human cyber security’ KPI kan dan een gewogen gemiddelde van de toename/afname score zijn waarbij een toename van een positieve onderliggend gedrag de waarde +1 krijgt, onveranderlijkheid de waarde 0 en een afname in positief gedrag de waarde -1 krijgt. Voor negatief gedrag moet de polarisatie worden omgekeerd. Een gewogen of rekenkundig gemiddelde over deze scores per gedraging levert een getal op tussen +1 en -1 en maakt in een oogopslag inzichtelijk of de gewenste gedragsverandering organisatie(deel)-breed heeft plaatsgevonden in een periode of juist niet.



Figuur 7-2 Voorbeeld van trend en verandering in human cyber security gedurende een fictief jaar.

Figuur 7-2 laat een fictieve human cyber security KPI trend zien. In de maanden maart, april, augustus, september, oktober en december laat de KPI zien dat het gewenste gedrag *toe*neemt. In de maanden januari en november laat deze grafiek zien dat het ongewenste gedrag toeneemt. Op deze wijze kan een organisatie vrij eenvoudig vaststellen of de genomen maatregelen bijdragen aan de cyber security naar aanleiding van het cyber secure gedrag van zijn gebruikers. De keuze voor de gedragingen die relevant zijn, zal afhankelijk zijn van de dan geldende dreigingen. In de huidige context zijn phishing en gebruik van ICT middelen voor zowel werk als privé de relevante dreigingen (zie van Vliet et al., 2017 en Paragraaf 8.2.2 van dit rapport). Welke dreigingen actueel zijn valt na te gaan via rapportages van bijvoorbeeld NCSC (Cybersecuritybeeld Nederland CSBN, 2018).

7.5 Conclusie

Samengevat, kan, om cyberveiligheid te beoordelen, gekeken worden naar het veiligheidsniveau van machines en naar het veiligheidsniveau van mensen. Wij houden ons hier bezig met het niveau bij mensen. Belangrijk is om vast te stellen wat het niveau is van de subjectieve beleving van cyberveiligheid. Hiertoe is de cyber security monitor ontwikkeld. Idealiter wordt dit aangevuld met KPI's die iets zeggen over het objectieve niveau van cyberveiligheid. Dit kan gemeten worden via bijvoorbeeld tellingen of logging van systeeminformatie.
Van uiterst belang bij het verkrijgen van inzicht in het niveau van cyberveiligheid is het idee dat het gaat om het meten van veranderingen. Daarom bevelen wij aan de KPI's periodiek te meten, bijvoorbeeld ieder jaar. Alleen dan is het mogelijk om iets te zeggen over van cyberveiligheid op een overkoepelend niveau en over de effecten die interventies teweeg brengen op concreet niveau.

8 Workshop Veilig Werken

8.1 Workshop

8.1.1 Deelnemers en programma

Op 28 juni 2018 is bij TNO Soesterberg is een workshop gehouden met 17 deelnemers van verschillende publieke en private organisaties, een paar van de personen die eerder geïnterviewd zijn waren in deze workshop ook aanwezig. Hiernaast waren er bij de workshop meerdere andere organisaties betrokken. Doelen van de workshop waren:

- Een evaluatie van de CSA. Dit had twee kanten:
  - het praktisch gebruik van de CSA: is de CSA begrijpelijk en gebruiksvriendelijk? Is de informatie nuttig en behulpzaam?);
  - de toepassing van de CSA (Helpt: helpt de CSA om de cybersecurity te vergroten?, Hoe zouden eindgebruikers het inzetten? Hoe zien ze de meerwaarde in de context van hun functie en organisatie?).
- De stakeholders op de hoogte te brengen van de ontwikkelingen in onze inhoudelijke visie.
- Identificeren van aspecten van de CSA die in een vervolgversie verbeterd kunnen worden.

De meeste deelnemers waren al bekend met ons werk op het gebied van Human Factors in Cybersecurity en hadden in april 2017 ook deelgenomen aan een door ons georganiseerde workshop. Een enkele deelnemer was ‘nieuw’ en was aanwezig omdat een genodigde hem/haar de uitnodiging had doorgestuurd. Tijdens de workshop hebben de deelnemers gewerkt met de tool en hebben ze in groepsdiscussies aan de hand van deze ervaring feedback gegeven.

8.1.2 Uitkomsten

Algemeen
Uit de workshop bleek dat de deelnemers enthousiast zijn over de CSA en dat ze in de opzet veel potentie zien. Tijdens de interactieve sessie hebben de deelnemers ongeveer 15 minuten met de tool gewerkt. In deze tijd heeft men de bestaande inhoud goed kunnen doornemen. Inhoudelijk is de tool op dit moment beperkt gevuld; het is een prototype. De deelnemers vonden de tool intuïtief in het gebruik. Wel vonden ze dat er relatief veel tekst aangeboden werd.

Gedragsanalyse
De ondersteuning die wordt geboden in het analyseren waarom medewerkers bepaald gedrag vertonen werd het meest gewaardeerd. Dit onderdeel sluit goed aan bij een behoefte die ze hebben. Men gaf aan dit in de praktijk lastig te vinden. De tool kan hen helpen de juiste vragen te stellen. Al zou men hier graag nog meer in begeleid worden.

Interventies
De gebruikers gaven aan graag veel meer en veel concretere interventies in de tool beschikbaar te hebben, al werd begrepen dat dit in dit prototype niet opgenomen was. Tijdens de discussie werd genoemd dat het voor toekomstig gebruik van de tool belangrijk is om regelmatig te zorgen voor voldoende nieuwe inhoud om gebruikers er toe te zetten de tool vaker ter ondersteuning te gebruiken. Dit kan door andere gedragingen toe te voegen, meerdere mogelijke interventies op te nemen en ook door ervaringen met elkaar te delen. Bijvoorbeeld door aan te geven

of een gebruikte interventie het gewenste effect gehad heeft. Dit sluit aan op een ander punt dat genoemd werd, namelijk dat de tool ingezet kon worden om een community te vormen, waarin men ervaringen met elkaar deelt.

Uitbreiden van de CSA
Voor organisaties is het daarnaast ook belangrijk de tool voor eigen gebruik uit te kunnen breiden en in te kunnen vullen. Bijvoorbeeld door interventies toe te voegen die binnen hun organisatie goed passen. Ook had men interesse in het vastleggen van meetgegevens over gekozen interventies binnen hun organisatie. In het kader van ‘meten is weten’ kan zo vastgelegd worden of de interventies het beoogde effect bereikt hebben. Dit is ook belangrijk voor besluitvorming van het hoger management in de organisaties. Inzicht in het effect van maatregelen helpt bij het toekennen van budgetten voor interventies om de cyber security te verbeteren en verantwoorden van de inzet van die budgetten.

Tailor made
Tijdens de workshop was er veel vraag naar hoe de CSA gepersonaliseerd kan worden per organisatie, welke mogelijkheden er zijn in de huidige opzet en hoe de tool aangevuld worden met lessons learned, ervaringen en mogelijk metingen. Met deze functionaliteiten zou de organisatie aan de hand van eigen richtlijnen de CSA kunnen invullen met interventies die daadwerkelijk toepasbaar zijn binnen de organisatie.

Push berichten
Om de CSA relevant te houden leek het de deelnemers handig dat er push berichten worden verzonden zodra er nieuwe content in de CSA is toegevoegd. Door push berichten en andere meldingen vanuit de CSA blijft men getriggerd om met de CSA te werken.

Community
De deelnemers gaven aan graag een community te realiseren binnen de eigen organisatie en daarbuiten, waarbinnen nieuwe interventies, ervaringen, lessons learned, resultaten, en metingen gedeeld kunnen worden. Maar een belangrijk aspect hiervan is ook om met elkaar de dialoog aan te kunnen gaan over hoe de cybersecurity problematiek aangepakt kan worden, rekening houdend met verschillende doelgroepen en snel veranderende dreigingen.

Risicoanalyse en verantwoording
De deelnemers vonden het belangrijk dat de CSA als instrument ingezet kan worden om het management te overtuigen van de noodzaak van een specifieke cyber security aanpak en de reden voor een bepaalde interventie. Daarom zouden de deelnemers het prettig vinden als er in de CSA een risicoanalyse stap toegevoegd kan worden. Met deze risicoanalyse kan men dan bepalen welk cyber onveilig gedrag de grootste risico’s met zich mee brengt. Het kan namelijk zo zijn dat bepaald cyber onveilig gedrag niet vaak voorkomt, maar dat de risico’s enorm groot zijn, terwijl een andere cyber onveilige gedraging heel vaak voorkomt, maar de risico’s klein zijn. Een organisatie moet afwegen waar het beste op in gezet kan worden.

Daar waar het binnen de beperkte middelen van dit project mogelijk is, zullen de bovengenoemde aanbevelingen worden meegenomen in een tweede versie van de CSA tool. Aanbevelingen die in het huidige project niet meegenomen kunnen worden, zullen in toekomstige projecten en initiatieven opgepakt moeten worden.

8.2 Vragenlijst cyberproblematieken

8.2.1 Vragenlijstitems

Als onderdeel van de Workshop Veilig Werken is voor aanvang van het formele programma een korte vragenlijst onder deelnemers uitgezet. Deze bevatte vier vragen:

1. *Hieronder staat een lijst met onveilige cybergedragingen. Welke cyber-gedragingen hebben volgens u bij uw bedrijf de hoogste prioriteit om aan te pakken? U kunt de top drie aangeven met een cijfer in de linker kolom. Indien u een cybergedrag mist, kunt u die onderaan in de lijst aanvullen.*

Prioriteit	Onveilig cybergedrag
	Downloaden onveilige bestanden
	Gebruik privé-middelen voor werkdoeleinden
	Verlies hardware
	Gebruik van onveilige netwerken
	Klikken op onveilige links
	Gebruik zelfde wachtwoord voor verschillende doeleinden
	Klikken op onveilige pop-up
	Bewust bezoeken onveilige websites
	Onbewust bezoeken onveilige websites
	Iets anders…

2. *Wat zorgt ervoor dat de aangegeven onveilige cybergedragingen de hoogste prioriteit hebben?* (open vraag)
3. *Wat zijn de redenen van het personeel voor het vertonen van het onveilige cybergedrag?* (open vraag)
4. *Wat zijn eventuele oplossingen zodat het onveilige cybergedrag niet meer vertoond wordt?* (open vraag)

8.2.2 Uitkomsten

Vraag 1: Wat zijn de top drie cybergedragingen met prioriteit?
De rangorde die de deelnemers aan de verschillende gedragingen gaven werden gescoord door het gedrag op nummer één 3 punten te geven, het gedrag op nummer twee 2 punten te geven, en het gedrag op nummer drie 1 punt te geven. De scores voor ieder gedrag zijn vervolgens opgeteld. Het gedrag met de hoogste score werd geïnterpreteerd als het meest prangende probleem. De scores per gedrag worden in Tabel 8-1 weergegeven.

Tabel 8-1 Frequenties van gekozen gedragingen en rangordening.

Onveilig cybergedrag	Score	Rang
Klikken op onveilige links	26	**1**
Gebruik privé-middelen voor werkdoeleinden	16	**2**
Downloaden onveilige bestanden	12	**3**
Gebruik van onveilige netwerken	9	4
Verlies hardware	8	5
Gebruik zelfde wachtwoord voor verschillende doeleinden	8	5
Klikken op onveilige pop-up	6	7
Bewust bezoeken onveilige websites	5	8
Onbewust bezoeken onveilige websites	2	9

De drie genoemde cybergedragingen met de hoogste prioriteit waren *Klikken op onveilige links, Gebruik IT middelen voor zowel privé als werkdoeleinden* en *Downloaden onveilige bestanden.* Dit komt overeen met de bevindingen van ons onderzoek in 2017.
In het geval van Vragen 2, 3 en 4 werden de antwoorden geanalyseerd door gemeenschappelijke thema's in de responsen te identificeren. De antwoorden zijn niet behandeld als zijnde specifiek per aangegeven respons maar als generieke antwoorden over dat onderwerp binnen organisaties.

8.2.2.1 *Vraag 2: Waarom hebben volgens u de door u aangegeven onveilige cybergedragingen de hoogste prioriteit?*

De meest voorkomende redenen voor prioritering waren:

1. Cybergedrag (bijvoorbeeld klikken op links, onveilige verbindingen) brengt veel risico's met zich mee
2. De impact van deze risicovolle gedragingen is groot als het fout gaat (bijvoorbeeld datalekkage, malware)

8.2.2.2 *Vraag 3: Waarom denkt u dat personeel van uw organisatie deze gedragingen doet?*

Tabel 8-2 geeft een samenvatting weer van de redenen die de experts gaven als verklaring voor onveilig cybergedrag van personeel:

Tabel 8-2 Samengevatte antwoorden op Vraag 3.

Reden	Toelichting
Men ziet het niet	• Onwetendheid • Onbewust dat er iets gebeurt • Onbewust van risico's • Niet expres

Wij zijn ook maar mensen	• Motivatie
	  ○ Slordigheid
	  ○ Nieuwsgierigheid
	• Cognitief
	  ○ Informatie overload
	  ○ Risico's moeilijk te herkennen
	  ○ Complexiteit (bijv. bij wachtwoorden)

Beleid	• Onduidelijkheid (over bijv. rol of regels) • Onveilig gedrag is toegestaan (bijv. inloggen op openbare WiFi)

Reden	Toelichting
	• Alternatieven worden niet geboden
Gemak	• Oftewel gemakzucht

Wat opvalt is de diversiteit aan redenen die opgegeven zijn. Het is niet alleen dat men veronderstelt dat gebruikers lui zijn of zich niet bewust zijn van de gevaren en wat veilig gedrag inhoudt.
Gemak is een interessante om bij stil te staan; deze is tevens vaak een aantal keer genoemd en houdt wellicht verband met redenen zoals *slordigheid*. Samengenomen, de opgegeven redenen lijken met elkaar samen te hangen. Mensen zien de risico's niet, mede omdat ze die niet begrijpen. Omdat ze ook maar mensen zijn, heerst er een idee dat ze er ook niets aan kunnen doen: ze zijn niet gemotiveerd om het te snappen en het is cognitief gezien ook erg moeilijk allemaal. De combinatie met 1) onduidelijk of ontoereikend beleid en 2) onbehulpzame/ onbegripvolle reactie vanuit IT beheer als iemand wel een keer de moeite neemt (bijvoorbeeld om een phishing mail te melden) helpen niet mee. De combinatie van dit alles leidt vervolgens tot gemakzucht. Dit is de uitkomst van het proces en houdt verband met het geven van prioriteit aan het behalen van een cyberdoel boven cyberveilig gedrag. En dit is zeker zonde omdat een werkgever de kans mist om zijn/haar medewerkers als sensoren in te zetten om malafide zaken te detecteren.

8.2.2.3 *Vraag 4: Wat zijn volgens u eventuele oplossingen zodat deze gedragingen niet meer vertoond worden?*

De antwoorden worden samengevat in Tabel 8-3.

Tabel 8-3 Samengevatte antwoorden op Vraag 4.

Reden	Toelichting
Bewustwording (al dan niet in combinatie met een technische oplossing)	• Voorlichting • Training • Oefenen met risico's (bijv. nep phishing mails)
Techniek	• Bepaalde handelingen onmogelijk maken/afdwingen (bijv. apparatuur dichttimmeren, complexe wachtwoorden vereisen) • Betere techniek achter de schermen (bijv. filters, anti-malware) • Mens ondersteunend (bijv. encryptie of multi-factor authenticatie)
Bedrijfscultuur	• Aanpassen/veranderen • Versterken
Overige	• Aanbieden veilige opties (bijv. ondersteunende tools, alternatieve inlogmethodes) • Monitoren • Risico accepteren

Een paar dingen vallen op in de responsen op Vraag 4. Ten eerste, verreweg het meest genoemd is het vergroten van bewustzijn (awareness) en trainingsniveau. Ten tweede zijn technische oplossingen, al dan niet in combinatie met het verhogen van bewustzijn, ook veel genoemd. Een aantal van deze technische oplossingen ging over het afdwingen van veilig gedrag en het onmogelijk maken van onveilig

gedrag. Hierbij is weinig rekening gehouden met de impact van deze afdwingende maatregelen op het vinden van omwegen om alsnog het gewenste gedragsdoel te behalen. Ten derde, een enkele keer is bedrijfscultuur genoemd: als de bedrijfscultuur in lijn is met cyberveilig handelen, zullen medewerkers hun gedrag aanpassen. Tenslotte, een aantal oplossingen was anders van aard, bijvoorbeeld het aanbieden van veilige opties en het monitoren van het niveau van cyberveiligheid in de organisatie.

8.2.3 Conclusies

De top drie prioriteitsgedragingen waren helder: klikken op onveilige links, gebruik van ICT middelen voor zowel privé- als werkdoeleinden en downloaden van onveilige bestanden. De redenen waarom deze in de top drie stonden waren duidelijk: deze gedragingen brengen veel risico's met zich mee en de impact ervan is groot.

Onze experts hebben redelijk kunnen nuanceren waarom mensen deze onveilige gedragingen vertonen. Ondanks het feit dat de deelnemers tijdens de workshop aangaven de gedragsanalyse moeilijk te vinden, laten de vragenlijstdata zien dat ze daar best vaardig in zijn; ze scheren alles zeker niet over een kam. De deelnemers geven aan dat de redenen te maken hebben met menselijke beperkingen in termen van informatieverwerking en motivatie, maar ook met beleid en organisatierichtlijnen, en de moeilijkheid van technische eisen.

In termen van de oplossingen zien wij minder differentiatie. Bovenaan de lijst staat het verhogen van cyberawareness. Verbeteren van techniek, en met name het technisch dichttimmeren van onveilige alternatieven volgt al heel snel. Opmerkelijk is dat binnen deze categorieën weinig concretisering is van de reacties. Er wordt bijvoorbeeld niet gesproken over concrete technische manieren om een systeem af te schermen. Dit kan mogelijk verklaard worden doordat de respondenten wellicht bang waren dat een te technisch antwoord niet begrepen zou worden door de (niet technisch onderlegde) organisatie van de workshop.

Het feit dat awareness zo vaak genoemd is als een soort van *one-size-fits-all* voor een diversiteit aan problemen lijkt erop te duiden dat respondenten óf awareness inderdaad als een panacee zien óf dat ze zich weinig andere oplossingen kunnen voorstellen. Dit is consistent met onze eigen bevindingen uit de literatuur en in de vele gespreken met stakeholders.

Ook interessant is dat hoewel het technisch dichttimmeren van gevaarlijke aspecten van systemen een inherent aantrekkelijke oplossing is, het geen rekening houdt met de creativiteit van mensen om toch dat wat zij willen doen voor elkaar te krijgen via een omweg.

Samengenomen, bevestigen deze bevindingen onze eigen conclusies over hoe organisaties momenteel over cyberveiligheid denken, namelijk 1) dat het probleem niet volledig terug te voeren is naar een gebrek aan bewustzijn en 2) dat op dit moment de gemeenschap geen adequaat alternatief heeft. Ook onderschrijft dit de noodzaak om op een andere manier over cyberveiligheid na te denken, namelijk vanuit het doel van de gebruiker en hoe de gebruiker via praktische, faciliterende interventies cyberveilig ondersteund kan worden.

9 Conclusie

Dit rapport beschrijft de activiteiten die uitgevoerd zijn in het kader van de eerste helft van dit project over cyberveilig gedrag?. De concrete onderzoeksvragen die in dit rapport onderzocht werden waren:

1 Waarom vertonen mensen onveilig cybergedrag en welke aanknopingspunten zijn er om cyberveilig gedrag te faciliteren?
2 Hoe kunnen diegenen die binnen organisaties verantwoordelijk voor cyberveiligheid ondersteund worden in dit proces?

In deze conclusie vatten we de antwoorden op de onderzoeksvragen samen.

9.1 Cyberonveilig gedrag

Onderzoek en praktijk komen steeds meer tot de conclusie dat het verhogen van het bewustzijn van hoe cyberveilig te handelen niet leidt tot veiliger cybergedrag. Wij veronderstellen dat mensen cyberonveilig handelen omdat cybergedrag niet een doel op zich is, maar een middel waarmee een ander gedragsdoel mogelijk wordt gemaakt. Belangrijk aanknopingspunt voor het verbeteren van de veiligheid van cybergedrag is om het gedragsdoel zo veel mogelijk in stand te houden en te faciliteren. In onze aanpak staat daarom centraal niet het expliciet veranderen van gedrag middels een bewust proces, maar het faciliteren van veilig gedrag door middel van het aanbieden van cyberveilige handelingsalternatieven zonder dat het doel waarmee mensen handelen gefrustreerd of geïnhibeerd wordt.
Wat ontbreekt in de bespreking van onze conceptuele ontwikkelingen is een discussie van de concepten *nudging, shoving* en *budging* (Oliver, 2017). Dit zijn concepten uit de gedragseconomie die verschillende mechanismes beschrijven die gebruikt kunnen worden in gedragsverandering en die relevant lijken te zijn voor onze visie. Toekomstig conceptueel onderzoek zou hier in meer detail naar kunnen kijken.

9.2 Ondersteuning

Om de kennis die ontwikkeld is naar de gebruikers te kunnen ontsluiten is gekozen voor de Cyber Secruity Assistent, een digitale tool die de gebruiker ondersteund in het identificeren van het cyberonveilige gedrag dat veranderd moet worden, begrijpen van de aard van dat gedrag en tenslotte het kiezen van een gepaste interventie om het gedragsdoel te faciliteren op een cyberveilige manier.
Het CSA concept is getoetst in interviews met stakeholders en het digitale prototype is in de Workshop Veilig Werken geëvalueerd.
In eerste instantie was voorgenomen om de structuur van de CSA te baseren op design patterns. Enerzijds zouden design patterns gebruikt worden om te helpen bij het identificeren van mogelijke interventies en anderzijds als manier om grote aantallen interventies gestructureerd te presenteren in de CSA. Voor wat betreft het eerste punt, omdat veel design patterns zich richten op het inhiberen van gedrag, vonden we deze niet geschikt voor de CSA omdat wij juist aanbevelen om zaken niet te verbieden maar te faciliteren. Voor wat betreft het gebruik van design patterns als structuur in de CSA, bleek dat er geen grote aantallen interventies geïdentificeerd konden worden, waardoor een structureringsmechanisme niet nodig was.

In de tweede helft van 2018 zal een tweede versie van de CSA worden gemaakt, waarin rekening gehouden wordt met de uitkomsten van de interviews en de workshop. Onderwerpen die aandacht zullen krijgen zijn bijvoorbeeld:

- De mogelijkheden om de CSA minder op tekst te baseren en meer op een grafische interface.
- De interventies die erin zijn opgenomen. Momenteel zijn veel interventies weinig inspirerend en nogal generiek. We zullen in de vervolgversie aandacht hebben voor concretere gedragingen, gepaard met concrete en creatieve interventies.
- De opname van aanwijzingen voor hoe de effecten van cybersecurity interventies te meten en te monitoren zijn.
- Adviezen voor informatie-uitwisseling, bijvoorbeeld een *repository* waar gebruikers zelf hun interventies en ervaringen kunnen toevoegen en mogelijk delen met andere CSA gebruikers.
- De mogelijkheid voor push-berichten waarbij de gebruiker geattendeerd wordt op de toevoeging van nieuwe inzichten of informatie.

Deze tweede versie van de CSA zal met een stakeholderorganisatie uitgebreid worden beproefd en geëvalueerd. De tweede versie van de CSA en resultaten van de beproeving worden in de volgende deelrapportage vastgelegd.

10 Literatuur

1. Accenture.com https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
2. Alexander, C. (1977). *A Pattern Language: Towns, Buildings, Construction.* Oxford University Press: New York.
3. Bada, M., Sasse, A., & Nurse, J.R.C. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? Proceedings International Conference on Cyber Security for Sustainable Society. (p. 118-131).
4. Barn, R., & Barn, B. (2016). An ontological representation of a taxonomy for cybercrime. In: *24th European Conference on Information Systems (ECIS 2016),* 12-15 June 2016, Istanbul, Turkey.
5. Cybersecuritybeeld Nederland CSBN 2018 (2018). Uitgave Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV).
6. IBM.com https://www.ibm.com/security/data-breach/threat-intelligence
7. Interaction Design Foundation, https://www.interaction-design.org/literature/article/10-great-sites-for-ui-design-patterns
8. Interaction Design Foundation, https://www.interaction-design.org/literature/topics/ui-design-patterns
9. Kapersky.com https://www.kaspersky.com/blog/the-human-factor-in-it-security/
10. Lockton, D., Harrison, D. and Stanton, N.A., Design with intent: 101 patterns for influencing behaviour through design, 2012 http://designwithintent.co.uk/docs/designwithintent_cards_1.0_draft_rev_sm.pdf%20.
11. Oliver, A. (2017). Nudges, shoves and budges: Behavioural economic policy frameworks. *J Health Plann Mgnt. 33*, 272-275.
12. RTL Nieuws (2018). *We eten veel te weinig groente maar hebben dat niet door,* https://www.rtlnieuws.nl/gezondheid/we-eten-veel-te-weinig-groente-maar-hebben-dat-niet-door
13. Sabillon, R., Cano, J., Cavaller, V., & Serra, J. (2016). Cybercrime and cybercriminals: a comprehensive study. *International journal of computer networks and communications security*, *4*(6), 165.
14. Suleman, I. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice, 44-57,* 47. doi.org/10.1016/j.ijlcj.2016.07.002.
15. Symantic-norton.com http://www.symantec-norton.com/11-most-common-computer-security-threats_k13.aspx
16. UI-patterns.com, http://ui-patterns.com/; http://ui-patterns.com/patterns
17. Usability v safety: how to design our way to better security, The Guardian, https://www.theguardian.com/media-network/2015/nov/26/usability-safety-how-to-design-better-security-technology
18. Vliet, T. van, Broekman, C., Hemert, D. van, Prins, S., Rijk, R. van, Wijn, R., Young, H., Brusselers, M., Coetsier, D., Hueting, T., Jol, S., Langefeld, A., & Verburgh, T. (2017). Human Factors in Cybersecurity: Een conceptueel raamwerk en empirische toepassingen. TNO Rapport nr. 2017 R11574. TNO Soesterberg.

19. Welie M. van, Veer, G.C. van der, & Eliens, A. (2001). Patterns as Tools for User Interface Design. In: *Tools for Working With Guidelines.*
20. Young, H.J., Wijn, R., Rijk, R. van (2018). Veilig cybergedrag: Niet veranderen maar faciliteren. *Beveiliging, jaargang 31, p.30-32,* https://view.publitas.com/security-press/beveiliging-april-2018
21. Youtube.com https://www.youtube.com/watch?v=2lXh2n0aPyw

A Overzicht onveilige cybergedragingen en interventies

De tabel hieronder geeft een overzicht van interventies die bij ons bekend zijn. De voorbeelden van bijbehorende interventies komen uit gesprekken met stakeholders, diverse websites en zijn op basis van eigen kennis en ervaring. Een paar kanttekeningen:

- Cyberawareness is belangrijk voor veilig cybergedrag; immers, zonder te weten wat er aan de hand is, kan niet van je verwacht worden dat je ernaar handelt. Het is volgens ons echter nooit afdoende. Awareness campagnes, andere voorlichtingsmethoden en training moeten altijd vergezeld gaan met faciliterende maatregelen.
- Wij geloven in de kracht van interventies die gedrag faciliteren en mogelijk maken. Interventies die gericht zijn om gedrag actief te blokkeren/voorkomen/ ontmoedigen zijn in onze visie minder effectief. In onderstaande tabel zijn met name faciliterende maatregelen weergegeven. Voor de volledigheid is ook een aantal blokkerende maatregelen opgenomen, al zouden wij deze maatregelen niet aanbevelen.

Tabel A.1 Risicogedragingen en voorbeelden van interventies.

Risicovolle gedraging	Voorbeelden van interventies
Niet updaten van software	– Gebruik automatische software updates
Downloaden van onveilige bestanden	– Websites om veiligheid van bestanden te checken zoals Virustotal.com
Installeren van onveilige programma's	– Websites om installer veiligheid te checken zoals Virustotal.com
Bezoeken van onbetrouwbare websites (bijv. via hyperlinks in een document, phishing mail, website)	– Websites om URL veiligheid te checken zoals URL Void of URL Scan (gratis) of Microsoft ATP Safe Links of Norton Safe Web (betaald). – Indien per ongeluk (bijv. in a phishing mail), laat emails van onbekende afzenders zien in platte tekst. – Spam filters. – Indien door nieuwsgierigheid, geeft links naar websites met lijsten van onveilige sites (zie hierboven).
Gebruik onveilige hardware of gebruik hardware op onveilige wijze	– Maak gebruik van Mobile Device Management (MDM) – Gebruik data blockers om mobiele telefoons op te laden aan andere hardware (bijv. Link). – Maak oplaadstations beschikbaar op strategische plekken in de organisatie. – USB scrubbers (e.g. Link) – Om frequentie te monitoren, verspreid USB sticks geconfigureerd met speciale software door het gebouw en registreer wanneer medewerkers de USB sticks gebruikt worden. – Gebruik software zoals Mobile Threat Defense (Motiv) voor de veiligheid van mobiele devices. (Detecteert

	kwaadaardige apps, blokkeert malware, beschermt tegen onveilige WiFi en blokkeert phishing via SMS) – Device managementsysteem waarin alleen geregistreerde devices op het netwerk kunnen inloggen. (Wij onderschrijven het gebruik van dergelijke onderdrukkende maatregelen niet; deze interventie wordt hier genoemd voor de volledigheid.)
Geven van confidentiële informatie via een onveilige methode.	– Gebruik encryptie – Gebruik een veilige informatietransfermethode, bijv. een door de organisatie goedgekeurde documenttransfertool. – Blokkeer het gebruik van programma's zoals dropbox en google docs. (Wederom wij onderschrijven dergelijke blokkerende maatregelen niet.) – Gebruik een veilige data/document transfertool.
Geven van confidentiële informatie aan een onbetrouwbare, externe of onbekende organisatie of person.	– Wanneer het een kopie betreft van een legitimatiedocument of ander gevoelig document, schrijf op de kopie dat het een kopie betreft die alleen gebruikt mag worden voor doeleinde X en dat het niet voor een ander doeleinde gebruikt mag worden.
Computer/device door een ander laten gebruiken.	– Maak gastenaccounts mogelijk
Verlies hardware	– Rust hardware uit met GPS trackingfunctionaliteit, zoals op mobiele telefoons.
Delen van wachtwoorden	– Zorg dat medewerkers toegang hebben tot alle voor hen relevante informatie, waardoor de behoefte om toegang te krijgen via de account van een college beperkt blijft. – Gebruik biometrics voor login – Gebruik een tool om gebruikersrechten te managen. – Gebruik een combinatie van methoden om logins te identificeren bijv. SMS, hardware tokens, software tokens, certificaten en adaptieve authenticatie.
Gebruik zelfde wachtwoord op verschillende accounts/systemen	– Gebruik een wachtwoordmanager – Gebruik biometrics voor login – Gebruik multi-factor authenticatie
Gebruik onveilige netwerk (geen netwerk is inherent onveilig, maar openbare netwerken brengen meer risico's met zich mee.)	– Gebruik VPN's, dongels, of 4G. – Gebruik mobiele telefoon als hotspot.
Gebruik privé mail voor werkdoeleinden	– Zorg dat medewerkers remote en veilige toegang hebben tot alle informatie die zijn nodig hebben om hun werk uit te voeren, inclusief hun email. – Gebruik een email veiligheidsprogramma die cyber-attacks die gebruik maken van e-mail ondervangt.

Verzaken een device op slot te zetten	– "Hack your colleague": Maak een rapportagefunctie die mensen kunnen gebruiken wanneer zij een ongelockte device zien. Hierdoor kan een device gelockt worden en kan een incidentrapportage gemaakt worden. Dit kan ook gegamificeerd worden.
Onvoldoende cyberawareness (wij adviseren cyberawareness te adresseren, al zijn wij van mening dat het niet afdoende is om veilig cybergedrag te bewerkstelligen en gebruikt moet worden in samenhang met andere interventies.)	– Kaartenspellen met do's & don'ts. – Muismatjes met informatie over cyberveilig gedrag – 'Mystery guests' – Serious games om awareness te verhogen. – Awarenesstraining inclusief e-learning, microlearning en het gebruik van ondersteunende tools – Nep phishing mail campagnes – Websites zoals Alert Online
Monitoring (zie ook Paragraaf 4.2 van dit rapport)	– Medewerker enquête over cybergedrag en veiligheidsperceptie. – Loggen van objectieve events (bijv. virusaanvallen, aantal gerapporteerde phishing mail) – Kwetsbaarheidsscanners die scannen voor risico's en zwakheden

Tabel A.2 Categorieën interventies uit: https://www.sspedi.co.uk/aisb2018

Category	Sub-category
Behaviour intervention methods and techniques for cyber-security	Methods and techniques for encouraging user education, user awareness, user compliance
	Methods and techniques for improving risk perception and risk-related behaviour
	Methods and techniques for dissuading criminal, anti-social and negligent behaviour
	Methods and techniques for persuading senior managers to own and manage risk
	Persuasion and deterrence
	Social aspects of persuasion
	Gamification
	Peripheral, ambient, and pervasive routes of persuasion for cyber-security
	Personalization of methods and techniques
	Personalization of the selection of methods and techniques
Persuasive argumentation for cyber-security	Generating persuasive arguments (identifying discourse goals, choosing argument structure, content selection)

	Persuasive discourse processing: understanding what users say in terms of argumentation schemes
	Computational models of argumentation
	Rhetoric and affect: the role of emotions, personalities, etc. in models of argumentation
	Enhancing receiver involvement
User, community and context models for digital behaviour interventions for cyber-security	Modelling attitudes, capabilities, and current behaviour (e.g., compliance, non-compliance)
	Modelling personality and affective state for persuasion
	Modelling cognitive load
	Analysis of sentiment, intention, topics and affective state to spot threats and risks
	Modelling security policies and procedures
	Effect of demographics, job roles, education and cultural differences on persuasion and cybersecurity
	Effect of community/organizational culture and task context
User-centred design and evaluation methodologies for digital behaviour interventions for cyber-security	
Persuasive User Interfaces for cyber-security	Use of (multiple) Embodied Conversational Agents for persuasion
	Communication settings (e.g. direct versus indirect communication)
	Timing of persuasive messages/ when to interrupt the user
	Effective presentation of communications
	Effective presentation of cyber-security data (e.g. visualisation)
	Effective interactions
Applications of digital behaviour interventions for cyber-security	Public and private sector cyber-security
	Citizen cyber-security
	Cyber-security across domains (e.g. somebody taking a device from work to home)
Ethical issues of digital behaviour interventions for cyber-security	
Privacy and trust issues for digital behaviour interventions for cyber-security	

B Design Patterns

De tabel hieronder geeft de verschillende design patterns weer die wij in acht hebben genomen. Meer detail over deze analyse is te vinden in Hoofdstuk 5.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
Converging & diverging	Architectural	Structure behaviour: users follow the designers' behaviour specification without necessarily being aware of it. Channel people to come together or split up.	Gates (and gatehouses) channel visitors through a narrow opening, allowing a toll to be levied, or to help control potential threats.	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
conveyor belts	Architectural	Bring a feature to the users, or move the users to where you want them to be	Moving walkways in airports help travelers move more quickly, but also prevent people blocking corridors, especially in groups	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
feature deletion	Architectural	Take away features you don't want people to use	Various politicians have proposed simply removing standby buttons from consumer electronic products, to reduce energy use	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
hiding things	Architectural	Hide functions or elements you'd prefer people didn't use	Church hall heating controls have been hidden (leaving only the timer accessible) to reduce errors by users unfamiliar with them.	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
positioning	Architectural	Rearrange things so people interact with them in the locations you want them to	Positioning pedestrian crossing push-button units on the right-hand side (UK) makes it more likely that users turn to notice oncoming traffic	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
roadblock	Architectural	Put things in users' way, so they take an alternative route, or adjust their speed	'Chicanes' can slow down drivers, pedestrians and cyclists; the crossing chicane prevents running or cyclingstraight across the road	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
segmentation & spacing	Architectural	Divide your system up into parts, so people only use one bit at a time	These individual seats replace a bench on the Paris Métro – spaced so that someone cannot	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
			lie down or occupy more than one	
choice editing	Errorproofing	Edit the choices presented to users so only the ones you want them to have are available	Choice editing can be driven by legislation, e.g. leaded 4-star petrol being phased out in the EU by 2000	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
interlock	Errorproofing	Set things up so one action can't be performed until another is completed. It just silently structures behaviour: users follow the designers' behaviour specification without necessarily being aware of it.	Most modern cash machines don't dispense cash until you remove your card, making it less likely you'll leave it behind. The interlock on a microwave door prevents using the oven with the door open, yet does not try to educate users as to why it is safer.	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
matched affordances	Errorproofing	Make parts fit only when the right way round, or only with the products they should do	The bevelled corner on SIM cards, memory cards and floppy disks ensures that they can't be inserted the wrong way round	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
task lock-in/out	Errorproofing	Keep a task going that needs to be, or prevent one being started inadvertently	To prevent accidentally engaging reverse gear, most gearboxes include a 'gate' over/under which the stick must be lifted or pressed.	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
bundling	Machiavellian	Include something you want users to do, along with something they want to do, so both get done	Crushing up pills or tablets in a spoonful of peanut butter can be a good way to get dogs to take medicines they would otherwise refuse	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
degrading performance	Machiavellian	Degrade the performance of a product or system until users comply with some behaviour change you want	Some Nokia phones allegedly sense when a 3rd-party battery is used and switch into a high-power mode so it runs out more quickly	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
forced dichtomy	Machiavellian	Configure a system so there is no 'middle ground' possible, and users must make a choice one way or the other	An even-numbered (e.g. four-point) rating scale does not allow a 'middle' value: it forces respondents into making a 'good or bad?' choice	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
coercive atmospherics	Security	Use ambient sensory effects (sound, light, smell, etc) to make it harder for users to behave in certain ways	Blue lighting is used in some pub- lic toilets (e.g. here, in Edinburgh) to discourage drug injection by making veins difficult to see	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
threat of injury	Security	Your design threatens to (or actually does) harm users who behave in the 'wrong' way	Spikes on walls—such as these stick-on plastic ones—can act as a deterrent to climbing or sitting, with varying effectiveness	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
threat of property	Security	Your design threatens to damage users' property if they use it the 'wrong' way	'Traffic control spikes' are an attempt to enforce one-way traffic at entrances to car parks (etc): the threat is made very clear	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
what you can do	Security	Give users different choices or access to functions depending on the capabilities they can demonstrate	give users different choices or access to functions depending on the capabilities they can demonstrate	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
what you have	Security	Give users options or access to different functions depending on their possession of a special tool, key, device or token	Access cards allow the issuer to restrict entrance to certain buildings or areas to whoever has a card with the right permissions	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
what you know	Security	Test what users know (information, passwords, etc) to give them access to different functions	test what users know (information, passwords, etc) to give them access to different functions	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
what you have done	Security	Change the options available to users based on their current or previous behaviour	'Teaching machine' textbooks allow students to progress in different orders depending on which concepts need more explanation	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
what you are	Security	Make different choices available to users depending on their location	Some supermarket trolleys have devices fitted to lock the wheels when taken outside a defined area, usually an adjacent car park	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
who or what you are	Security	Use criteria innate to particular individuals, groups or objects to block or make different options available	Artificial height restrictors attempt to allow only certain types of vehicles into a car park, by discriminating on vehicle height	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
mazes	Architectural	Get people to follow the path you want them to, on the way to reaching something they want	Some store layouts route or channel shoppers past 'impulse purchase' items—often snacks—on their way to the checkouts	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
simplicity	Architectural	Simply structure things, to make it easier for users to do what you'd like them to do	EcoButton allows a user to put a computer into a low-power state with just one press, making it much easier for users to save energy.	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
defaults	Errorproofing	Make the default setting the behaviour you'd prefer users to perform	the default button (pressed if the user just hits 'enter') is more information on licensing rather than only 'I agree'	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
opt-outs	Errorproofing	Make an option something people opt out of, rather than opt in to	A building society asks new savers if they want to opt out of donating part of their interest to charity – by default it is donated	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
portions	Errorproofing	Change the size of the portions or the units of 'stuff' you give users	'Portion packs' for snacks give customers the 'right' amount of food to eat in one go (sometimes a particular amount of calories	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
partial completion	Interaction	Show that the first stage of a process has been completed already, to give users confidence to do the next	Pre-filled details such as delivery addresses can be an effective way of speeding up an order process and reducing 'shopping cart abandonment	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
tunnelling & wizards	Interaction	Offer users a wizard to 'tunnel' them through a decision process in the way you'd like	An installation wizard tries to get users to 'choose' to install additional (and irrelevant) software by presenting them as default parts of the process	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
make it a meme	Ludic	Plan your design to be something people want to spread, and make it easy for them to do so	ShareThis and similar quick access social sharing services can mean rapid 'viral' or 'meme' status for interesting or amusing stories	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
rewards	Ludic	Encourage users to take up or continue a behaviour by rewarding it, through the design of the system	Kai's Power Tools (pioneering visual effects software) revealed 'bonus functions' to reward users who developed their skill level	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
unpredictable reinforcement	Ludic	Give rewards or feedback on an unpredictable schedule, so users keep playing or interacting	Arcade games such as this coin pusher usually employ a strong element of unpredictable reinforcement, to keep users playing/paying	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
colour associations	Perceptual	Use colour to suggest associations between particular behaviours and outcomes	A racecourse bookmaker's keyboard has a detailed language of colour-coded groups of functions, to aid rapid action-taking	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
contrast	Perceptual	Create an obvious contrast between parts of your design or the context in which it's used	In 2004, Britain's Royal Mail switched to using red rubber bands for bundling post, to make them easier to spot if dropped accidentally	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
implied sequences	Perceptual	Make it look like there's a sequence for users to follow, through the layout of elements	This East German rail ticket machine makes very clear the order in which the interface should be used, with a sequential layout	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
mood	Perceptual	Use colour, images or other sensory stimuli to set a particular mood for a user's interaction with your system	Changes in hue, saturation and brightness can set moods: which room would you choose to stay in? (assuming the bed was made!)	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
perceived affordances	Perceptual	Design the form of your system to suggest particular actions (or constraints on action) to users	Reshaping the holes on bins to match the 'form' of different types of waste has been shown to increase recycling levels significantly	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
prominence	Perceptual	Direct your users' attention to what you want, by making it more prominent, obvious or exaggerated	The 'big red button' is a common way of making a control prominent. Here on London's DLR, it is recessed to help avoid accidental presses	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
proximity & grouping	Perceptual	Group elements so that users perceive they have similar functions or should be used together	This power supply has controls often used in pairs (coarse & fine voltage adjustment, and output terminals) explicitly grouped	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
similaritiy	Perceptual	Make elements look similar so users perceive them to share characteristics, or that they should be used together	Paid-for links on Microsoft's Bing look very similar to the real search results, to increase the chance of users clicking them	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
decoys	Cognitive	Add 'decoy' choices, making the others (which you want people to pick) look better in comparison	Would you choose the a $79.88 option, when the other two options offer you a free gift AND save you slightly more money?	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
do as you are told	Cognitive	Use an authority figure or authoritative instruction to tell users what they should (or should not) do	Impenetrable 'agreements' often make heavy use of authority (and threats) to reinforce their message: do as you're told	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
expert choice	Cognitive	Show users the choices that an expert or authority figure would make when in the same situation they're in	Endorsements where the celebrity is an 'expert' (such as chef Heston Blumenthal in this Waitrose campaign) can lend credibility	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
framing	Cognitive	Selectively present choices in a way which frames the range available in a more positive light	Starbucks' drink sizes start with 'tall', framing the range further up the scale and avoiding any mediocre implications of 'small' or 'medium'	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
scarcity	Cognitive	Emphasise that a resource is valuable, limited in quantity, or running out (or actually limit it artificially)	emphasise that a resource is valuable, limited in quantity, or running out (or actually limit it artificially)	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
social proof	Cognitive	Show people what other users like them are doing in this situation, and which choices are most popular	Amazon's recommendations can be helpful to buyers by expanding the scope of their knowledge, while increasing sales for Amazon	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
anchoring	Machiavellian	Affect users' expectations or assumptions by controlling the reference points they have	Restaurant menus may use 'anchor' items: prominently placed, higher-priced dishes, raising what customers expect to be paying	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
serving suggestion	Machiavellian	Direct users to use a product or system in a particular way through examples or demonstrations	Alka-Seltzer reputedly introduced the 'two tablets per dose' direction to users as part of a 1960s TV ad; before that, only one was taken	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
style obsolescence	Machiavellian	Design things to become unfashionable or undesirable quickly, to spur the desire for replacement or upgrades	Fashions and trends are obvious in high-street retailing, but are also prevalent (and can be deliberately created) in other fields	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
worry resolution	Machiavellian	Help users overcome worry about their behaviour (perhaps after having suggested it in the first place)	The term 'halitosis' was allegedly introduced in a 1921 Listerine ad, part of a series making people worried about bad breath, then offering a solution	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
explore/understand implications	Machiavellian	Knowing when it's appropriate to assume that users are being mindful of their behaviour, and when they're not, will be important for the 'success' of a design.	Thoughtful users are assumed to think about what they are doing, and why, and change their attitudes and behaviour in response to reasoned arguments, weight of evidence, education and persuasive rhetoric. If you model your users this way, you'll be looking to provide them with reasons why some behaviours are 'better' than others, maybe motivating them to change their attitudes about a subject as a precursor to changing their behaviour mindfully.	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
conditional warnings	Errorproofing	Give users warnings based on detecting the error they've made, or might be about to make	The parking brake warning light on a car's dashboard is a warning to the driver: don't drive off without releasing the brake!	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
did you mean?	Errorproofing	Detect and suggest a better option to users when it looks like they're making an error	Google's suggestion algorithm is continually evolving to take account of search trends; it also includes this nice 'easter egg'!	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
are you sure?	Errorproofing	Design an extra 'confirmation' step before an action can be performed	Some British Rail train doors require passengers to lower the window to get access to the handle, mounted on the outside	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
feedback through form	Interaction	Use the form of your object itself as a kind of interface, giving feedback or suggestive cues	Royal VKB's 100g/250g Balancing Bowls are weighted so they tilt noticeably and audibly when the 'portion size' is reached when filling	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
kairos	Interaction	Give users a suggestion at exactly the right moment for them to change their behaviour	Automatic warning signs can alert drivers to upcoming dangers at the right point for them to respond and slow down accordingly	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
peer-feedback	Interaction	Give users feedback on their behaviour from other users of the	Peer feedback on comments and stories is central to sites such as Slashdot ('karma'	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
		system, equal in status to themselves	scores) and Digg (’digging’ and ‘burying’)	
real-time feedback	Interaction	Let users know how what they’re doing is affecting the system	Energy meters can allow house-holders to see which appliances use the most electricity, and how much this is costing	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
simulation & feedback	Interaction	Give users a preview or simulation of the results of different actions or choices	Various politicians have proposed simply removing standby buttons from consumer electronic products, to reduce energy use	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
summary feedback	Interaction	Give users a report on what they’ve been doing, or its effects	GreenPrint, software that reduces wasted prints through better usability, provides users (and their bosses!) with a summary of resources saved	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
leave gaps to fill	Ludic	Leave deliberate gaps (in a design, message, etc) which users will want to fill, becoming engaged in the process	Deliberate use of red links on Wikipedia, signifying articles which should be written, “encourage[s] new contributors in useful directions”	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
role-playing	Ludic	System gives users particular roles to play, or makes them feel like they’re playing a role	Tim Holley’s Tio encourages children to become ‘energy champions’ for their household, influencing parental behaviour	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
storytelling	Ludic	Tell a story via your design, which interests users and keeps them engaged	Dyson uses narrative booklets drawing customers (and potential customers) into the story behind the company and its technology	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
nakedness	Perceptual	Remove cues that people take for granted, to get them to think more about what they’re doing	‘Naked roads’ with signage and markings removed can encourage pedestrians, cyclists and drivers to be more aware of each other’s presenc	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
watermarking	Perceptual	Make a user feel like he or she (or someone else) ‘owns’ or has responsibility for something	One UK shopkeeper writes customers’ names on the packaging of snacks they buy, discouraging littering through ‘taking ownership’	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
emotional engagement	Cognitive	Design your system to engage people's emotions, or make them emotionally connected to their behaviour	The open beak of a 'baby bird' litter bin at a city farm (visited by lots of children) suggests that they are hungry and would like to be fed	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
provoke empathy	Cognitive	Help users see other people's perspectives and thought processes, by revealing them through the design of your system	Twitter, Facebook et al allow us to see at any moment the problems and concerns of millions of others just like us (or not) all over the world	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
i cut, you choose	Machiavellian	Structure a system so that no one user can get an advantage over others simply by being first to act	If person 1 cuts a cake into halves, and person 2 chooses the half he or she wants, there is no advantage in person 1 cutting the cake unfairly	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
surveillance	Security	Inform users (or believe) that their behaviour is visible to or monitored by people in positions of power / authority	CCTV is often presented as a crime deterrent, influencing public behaviour, whether or not it is switched on or actually monitored	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
peerveillance	Security	Inform users (or believe) that what they're doing is visible to their peers also using the system	Neighbourhood Watch schemes are signed so that they provide a deterrent effect—"people here are vigilant about what's going on"	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
sousveillance	Security	Give people 'lower down' a hierarchy the ability to observe and monitor the behaviour of people above them	give people 'lower down' a hierarchy the ability to observe and monitor the behaviour of people above them	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
angles	Architectural	Angle things so some actions are easier than others	Some cigarette bins are sold to authorities using the sloping top as a feature, discouraging people leaving litter on top	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
material properties	Architectural	Use the properties of different materials to make some actions more	Rough-textured paving can act as a subtle barrier between cycle and pedestrian tracks:	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
		comfortable than others	stray over the line on a bike and you'll feel it	
pave the cowpaths	Architectural	Recognise the 'desire paths' of some of your users, and then codify them into your system, so others follow too	In Tigard, OR, residents marked informal 'neighbourhood trails' they used on a map, so the city could prioritise ones to 'formalise'	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
progress bar	Interaction	Let users know their progress towards achieving a goal	As demonstrated by examples from LinkedIn and Wikipedia, progress bars showing 'nearly complete' can make a goal seem more achievable	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
tailporing	Interaction	The systems adapts what it offers to match individual users' needs and abilities	The Pam personal activity monitor suggests exercise regimes tailored to the user—something approaching the role of a 'personal trainer'	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
challenges & targets	Ludic	Set people a challenge, or give them a target to reach through what they're doing	Whoever laid out this coffee tub as a target for throwing coins knew a lot about influencing people to donate generously and enjoy it. Make it a challenge/competition/game.	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
collections	Ludic	Encourage users to collect a set of things (friends, activities, places, objects, etc) through using your system	UbiFit Garden encourages users to maintain a regular variety of exercise activities, in order to 'collect' different types of flower	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
levels	Ludic	Split your system up into achievable levels which help users feel like they're making progress	Easy-to-reach levels lower the barriers to participation and encourage continued engagement for games such as FarmVille	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
playfullness	Ludic	Design something which 'plays' with its users, provoking curiosity or making interactions into a game	Spiral wishing wells turn giving money to charity into something actively fun for donors, and provoke curiosity of passers-by	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
scores	Ludic	Give users feedback on their actions as a score or rating allowing comparison to a reference point	The 'Brain Age' score given by Dr Kawashima's games for Nintendo gives users a clear incentive to keep using the software	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
symmetry	Perceptual	Use symmetry to make elements look related, or asymmetry to show difference and focus attention	The symmetrical holes on this lifebuoy, even without the text, suggest that it should be gripped with both hands simultaneously	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
fake affordances	Perceptual	Making something look like it works one way, while actually doing something else (or nothing at all)?	Many elevator/lift 'door close' buttons are reputedly 'placebo buttons', giving an illusion of control but not speeding up the process	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
methaphors	Perceptual	Employ a metaphor / analogy of something familiar, so people understand or use your system the same way	Tipjar.com, launched in the late 1990s, was one of the first simple micropayment systems, using the familiar metaphor of a tip jar	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
mimicry & mirroring	Perceptual	Make your system mirror or mimic a user's behaviour or mood in some way, to increase the engagement a user feels	Chatbots have evolved beyond the classic ELIZA, and are being used in social engineering attacks to extract information and deliver malware	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
possibilities trees	Perceptual	Give people a 'map' of the routes or choices they can use to achieve different goals	Presenting a simplified set of possibilities, transport maps can influence users' perceptions of geography, and promote certain routes over others	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
seductive atmospherics	Perceptual	Use ambient sensory effects (sound, light, smell, etc) to encourage users to interact or behave in the way you'd like	The distinctive 'Subway smell' may only be a by-product of baking, but intentional 'scent branding' is increasingly common in retail design	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
transparency	Perceptual	Reveal what's going on under the surface, to influence users' perceptions and behaviour	Dyson's transparent dust container both demonstrates the vacuum cleaner's effectiveness, and makes it likely to be emptied more often	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
assuaging guilt	Cognitive	Influence users by helping them reduce feelings of guilt about their behaviour	This message both implies that one should feel bad about the ethics of coffee production, and offers an easy way to take away the guilt: our coffee won't leave a bitter taste in your mouth. It's Fairtrade.	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
commitment & consistence	Cognitive	Get users to commit to an idea or goal, so they feel they should behave consistently with this commitment	In a 1976 study, householders sent a 'We are saving oil' sticker subsequently used 10% less heating oil than groups not sent the sticker	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
desire for order	Cognitive	Use people's desire for tidiness to influence them to rearrange elements or take actions you want them to	The AWARE Puzzle Switch, a light switch design by Loove Broms and Karin Ehrnberger, is visibly 'disordered' when in the 'on' position	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
habits	Cognitive	Make it easy for a new behaviour to become habitual, by building it into an existing routine	Simply choosing to take the stairs rather than the lift / elevator can quickly become part of a daily routine at home or work	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
personality	Cognitive	Give your system a personality or character that engages users, becoming a 'social actor'	Dutch researchers have used Philips' iCat robot to influence users' decisionmaking with washing machines, advising and expressing opinions	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
reciprocation	Cognitive	Make users feel they've been done a favour (by the system, or by other users) and want to return it	A busker's postcards may be 'free', but the social norms of reciprocation mean most people will give him some tip in return	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
rephrasing & renaming	Cognitive	Rephrase or rename what you'd like users to do, so it aligns better with what they already want to do	Twitter changed the name of the 'Devices' tab to the more easily understandable 'Mobile' to encourage more users to set up their phones	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
Antifeatures & crippleware	Machiavellian	Deliberately disable some functions even though they're still present, to drive users to upgrade, or to allow price discrimination	Sony's cheaper 60-minute MiniDiscs were identical to the 74-minute ones except for a pre-written portion of code preventing full use of the space	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
first one free	Machiavellian	Give something away which gets people interested or addicted, so they come back and pay for more	Offering one chapter (often the introduction) free has become increasingly common as a way of promoting new books more widely	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
forces dichotomy	Machiavellian	Configure a system so there is no 'middle ground' possible, and users must make a choice one way or the other	An even-numbered (e.g. four-point) rating scale does not allow a 'middle' value: it forces respondents into making a 'good or bad?' choice	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
format lock-in/out	Machiavellian	Design your system so users become committed to a particular format or way of doing things	Panasonic cameras include a 'battery authentication' system, which prevents using cheaper non-Panasonic replacements	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
functional obsolescence	Machiavellian	Design things to become technologically superseded (or even wear out) quickly, so people replace them	While new models do bring real technological advances, Apple has managed to create an 'upgrade treadmill' for iPhone buyers	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
poison pill	Machiavellian	Arrange things so that an otherwise attractive option has an unpleasant, self-defeating deterrent side-effect	Security ink tags release indelible ink if removed incorrectly, in an attempt to make it simply not worth stealing the clothes	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.
slow/no response	Machiavellian	Get users to try different actions or repeat a behaviour by making the system respond or give feedback slowly	Duplicate orders can be a problem where web forms are slow to submit and users click multiple times: this kind of instruction is common	Lockton, D. (2010). *Design with intent: 101 patterns for influencing behaviour through design*. Equifine.

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
Loss Aversion	Loss Aversion	Our fear of losing motivates us more than the prospect of gaining something of equal value	Use when a decision can be framed as either a gain or loss Use when you want to motivate the user to continue Use when you want to motivate the user to start	http://ui-patterns.com/patterns
Status-Quo Bias	Loss Aversion	We tend to accept the default option instead of comparing the actual benefit to the actual cost	Use when you want the user to choose the default option you want them to Use when you are making changes to your offering and want to keep users as your customers.	http://ui-patterns.com/patterns
Negativity bias	Loss Aversion	We have a tendency to pay more attention and give more weight to negative than positive experiences or other kinds of information.	We pay more attention and give more weight to negative feedback than positive. As we've seen with loss aversion, we work much harder to avoid losing $100 than we will work to gain the same amount – and painful experiences (loss) are much more memorable than pleasurable ones (gain). But whereas loss aversion refers to negative values, the negativity bias refers to negative information.	http://ui-patterns.com/patterns
Endowment Effect	Loss Aversion	We place greater value on objects we own over objects we do not, especially if sentimental value has been placed in them	Use when you want to let users place more value in your product than the one of a competitor. In a university study, students were parted into two equally sized groups. One group was given mugs ("seller"•) and the other ("chooser"•) nothing. When asked, the sellers in average wanted $7.00 for the mug, whereas the choosers were only willing to pay $3.50. The mug was evaluated as a gain by the choosers and as a loss by the sellers.	http://ui-patterns.com/patterns
Framing	Loss Aversion	We tend to avoid risk when a positive frame is presented but seek risks when	We determine value by comparing and contrasting things. The value of particular items can seem very different in	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
		a negative frame is presented	various situations, depending on the comparison. An implied story makes more desirable choices seem obvious.	
Optimism Bias	Loss Aversion	We consistently overstate expected success and downplay expected failure	When comparing ourselves to our peers, we tend to overestimate our future success and downplay our future failure. Limit the effect by highlighting possible losses using other biases, such as Loss Aversion. Make negative effects of critical actions clear to the user and offer a straightforward and safer alternative.	http://ui-patterns.com/patterns
Ilusion of control	Other cognitive biases	We have a tendency to believe that outcomes can be controlled, or at least influenced, when they clearly cannot.	Use when you want to motivate the user to strive for a goal. As humans, we have a desire to believe that we are in control and thus have a tendency to believe that outcomes can be controlled, or at least influenced, when they clearly cannot.	http://ui-patterns.com/patterns
Need for closure	Other cognitive biases	We have a desire for definite cognitive closure as opposed to enduring ambiguity.	Motivate your users by providing subtle cues to completion. Use when you want to motivate users to act. Do not use to motivate your users if what you want to motivate them to is cumbersome, enduring or cannot be achieved though small successes.	http://ui-patterns.com/patterns
Peak-end rule	Other cognitive biases	We primarily judge past experiences on how they were at their peak and how they ended	An interesting twist to the peak-end rule was found when it came to measuring the experienced discomfort of pain. Consider the series 2-5-8 and 2-5-8-4 in which the numbers refer to reports of pain provided on a 10-point scale every 5 minutes. Rationally, adding 5 extra minutes of pain will only increase total discomfort,	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
			although experiments showed the longer period of pain (20 minutes), but with a period of diminished discomfort in the end, were rated less discomforting than the shorter period of pain (15 minutes), but with an increased discomfort in the end.	
Curiosity	Other cognitive biases	We crave more when teased with a small bit of interesting information	Reveal just enough to arouse interest and tease users into taking action to reveal more. Users want to fill the information gap, and your job is to delay filling the gap for as long as you can without introducing too much discomfort. Keep them hanging on.	http://ui-patterns.com/patterns
Set Completion	Other cognitive biases	We desire collecting all pieces of a set more the closer it is to being complete	Completing a set of logically grouped tasks or items allows for achievable goals and small successes. Consider how you can have multiple levels of sets and what kind of things or information suggests logically grouped sets and set completion. This principle also applies to other things left incomplete such as puzzles, pictures, or sentences.	http://ui-patterns.com/patterns
Value attribution	Other cognitive biases	We tend to attribute the value, goodness, or authenticity of something to its context instead of the thing itself	We have a tendency to attribute people or objects with certain qualities based on perceived value rather than objective data. A high price may induce perceived qualities not seen if priced lower. An attractive appearance may induce a perception that a product works better.	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
Scarcity	Scarcity	If something is promoted as being scarce, we perceive it as more desirable and more valuable	Use when you want to convey a feeling of exclusivity Use when you want users to rush their decision Use when you want users to infer value in something Use when you want to encourage purchasing or other behaviour. Use when you want to precent users to take time to think about their decision, and instead push them into making a decision, immediately.	http://ui-patterns.com/patterns
Limited choice	Scarcity	We are more likely to make a decision when there are fewer options to choose from	How many choices do you offer? Can this be reduced? Every time you make it easier for users to think, they are more likely to make a decision. Simplify decision paths and present the more complex choices first.	http://ui-patterns.com/patterns
Limited duration	Scarcity	Use time limitations to push users to take action	Use limited duration offers to push users to make a decision now rather than later Use to force decision making to happen now rather than later Use to force comparison of possible options, based on the facts known during the limited time rather than after.	http://ui-patterns.com/patterns
Appropriate challenge	Gameplay design	The user needs appropriate challenges to remain engaged	Use when challenging users with too hard tasks will leave them stressed and full of anxiety Use when experienced users might be bored by too easy and mundane tasks. Use when the same system need cater to both experienced and unexperienced users.	http://ui-patterns.com/patterns
Levels	Gameplay design	Use levels to communicate progress and gauge users' personal development	As users progress, so does their skill level, requiring increasingly more difficult challenges.	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
Storytelling	Gameplay design	Use the narrative qualities of storytelling to let the user engage in a perspective	All our decisions are filtered through a story, whether it is real or imagined. Stories can be explicit and simple narratives or implied in the words you use. Suggest narrative elements like conflict, heroes, and villains.	http://ui-patterns.com/patterns
Intentional gaps	Gameplay design	Create intentional gaps that users can't help but try to fill	Leave deliberate gaps that users will want to fill. We are motivated to complete the incomplete. The closer to completion users perceive a task to be, the more motivated they are to finish it.	http://ui-patterns.com/patterns
Fixed rewards	Fundamentals of rewards	Use rewards to encourage continuation or introduction of wanted behaviour	When you invite friends to join dropbox.com and those friends end up creating an account, you are rewarded with extra space in your dropbox folder. The reward of prolonged play provide a great incentive to refer friends to use the dropbox.com service.	http://ui-patterns.com/patterns
Variable rewards	Fundamentals of rewards	Use random rewards to convey a sense of scarcity and unpredictability to entice users curiosity in discovering the pattern	Use variable rewards rather than fixed rewards when there is a chance that users will get acclimated to rewards the more they receive them.	http://ui-patterns.com/patterns
Completion	Gameplay rewards	Provide a feeling of closure by rewarding users at the completion of a goal	When you've completed the digg.com sign up process, the completion of the process is communicated as a victory, where after the next levels or objectives of the "game" are presented.	http://ui-patterns.com/patterns
Prolonged play	Gameplay rewards	Reward users by prolonging their game time to allow for higher scores and measures of success	Dropbox.com lurkes new users in by offering more space for each new referred customer. This clever game mechanic is called Prolonged play.	http://ui-patterns.com/patterns
Powers	Gameplay rewards	Give users a way to reach their goal	This user on stackoverflow.com has a flag weight of 145 - actions of this user will weigh	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
		more quickly than they could before.	much more than the actions of a newly signed up user.	
Praise	Gameplay rewards	Use explicit statements, graphics, a sound effect, or similar indicator to reward a job well done.	When you verify your tumblr.com account by clicking on a verification link in an email, your behaviour is praised.	http://ui-patterns.com/patterns
Unlock features	Gameplay rewards	Utilize a user's desire to explore by unlocking new features as a reward for specific behaviours	As you rise in rank on ConceptFeedback to become Elite or Titan member, you unlock the ability to have concepts posted in the "Premium concepts" section.	http://ui-patterns.com/patterns
Achievements	Gameplay rewards	We are engaged by activities in which meaningful achievements are recognized	What challenges and desired behaviour do you have in place and how are they linked to achievements? We are motivated by achievements of personal or social significance. In gaming, achievements are shown through points, badges, and levels; in other contexts through promotions, memberships, privileges, and acquisitions.	http://ui-patterns.com/patterns
Delighters	Gameplay rewards	We remember and respond favourably to new, unexpected, and playful pleasures	Delighters are the happy surprise that can make a difference, and an important source of satisfaction. If delighters aren't there, dissatisfaction and frustration won't follow: they're not expected.	http://ui-patterns.com/patterns
Reduction	Attention	Reduce complex behaviour to simple tasks, increasing the benefit/cost ratio and in turn influencing users to perform	Google reduces meaningful search on the web to something simple by relying on what was highlighted by other websites via back-links as being the most relevant for the user.	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
Tunnelling	Attention	Guiding users through a process or experience provides opportunities to persuade along the way	When you join last.fm, the chrome layout of the sign up form page is radically different from the chrome of the main site itself. All menu items and other links that will distract attention from signing up has been stripped away to tunnel the user toward the goal of signing up.	http://ui-patterns.com/patterns
Isolation Effect	Attention	Items that stand out from their peers are more memorable	You read the Plus section first because of Von Restorff Effect (Isolation Effect)	http://ui-patterns.com/patterns
Recognition over recall	Comprehension	We are better at recognizing things previously experienced than we are at recalling them from memory	When signing up for Pinterest, the Recognition over recall pattern is used to ask for the user's interests.	http://ui-patterns.com/patterns
Chunking	Comprehension	Information grouped into familiar, manageable units is more easily processed and remembered	When you enter a phone number into your iPhone, the phone number is automatically chunked into smaller bits of information that makes it easier for the user to read and remember. Breaking down the full phone number into more logical• chunks makes the number easier to remember.	http://ui-patterns.com/patterns
Sequencing	Comprehension	It is easier to take action when complex activities are broken down into smaller and more manageable tasks.	Break down complex tasks into small and easily completed actions, and set expectations as to how many steps are left before the entire sequence has been completed.	http://ui-patterns.com/patterns
Conceptual metaphor	Comprehension	We understand a new idea or concept by linking it to another.	Explain difficult concepts by making analogies.	http://ui-patterns.com/patterns
Anchoring	Comprehension	When making decisions, we rely, or anchor, too heavily on one piece of information.	Use when you want to make a price seem more fair or cheap – compared to the anchor Use when you want to control expectations of users as to how much to give, pay, or receive	http://ui-patterns.com/patterns
Pattern recognition	Comprehension	Even when there is no pattern, we seek	Make a game of arranging things in a manner that sparks	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
		ways to organize and simplify complex information.	curiosity and encourages pattern-seeking behaviour.	
Serial Positioning Effect	Comprehension	We have a tendency to recall the first and the last items in a series best.	The recency effect disappears when people think about other matters for thirty seconds after the last item in the list is presented.	http://ui-patterns.com/patterns
Kairos	Timing	Kairos represents situations of change. Situations of change are potentially valuable because they represent moments where users are open and receptive to making a deal or changing a behaviour.	Kairos occur in many situations – some are random but others come in patterns. One such pattern is when a user exits one group to join another. Such situations are potentially valuable as they represent moments where users are open and receptive to making a deal or making a behaviour change.	http://ui-patterns.com/patterns
Feedback loops	Timing	Every action creates an equal opposite reaction. When reactions loop back to affect themselves, a feedback loop is created.	Provide measures toward letting users know how what they are doing is affecting the system. This in turn allows users to adjust their behaviour and future actions toward reaching a greater goal.	http://ui-patterns.com/patterns
Tailoring	Timing	Tailored information is more effective in changing attitudes and beliefs than generic information. Make life simpler for users by showing only what is relevant to them. Tailor to individual needs, interests, personality, usage context, or other factors relevant to the individual.	Tailor information to users individually. Content will be more persuasive if it is tailored to the individual needs, interests, personality, or usage context.	http://ui-patterns.com/patterns
Trigger	Timing	Triggers cue the user to take action	riggers might be notifications, tweets, emails, text messages,	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
		in the context they are in.	links, or other distractions. Offline triggers should also be considered. Triggers can be set (alarms), brought home (printed reminder sheet), or follow an action (ask someone a question).	
Simulation	Timing	Simulation enables users to observe the link between cause and effect in real time. The rules used to simulate outcomes are based on assumptions and as such have persuasive power. Simulation can serve as a great learning tool, as it enables users to try out behaviour they wouldn't dare in the real world.	Let users play with and learn your system without the fear of messing up.	http://ui-patterns.com/patterns
Authority	Social Biases	We have a sense of duty to authority that makes us unable to defy their wishes. Authority help define the role we take upon ourselves and the roles we put on others. If an authority figure is seen as a teacher, we put on the learner or student role. If a policeman approaches us we take on the role as a suspect or informer.	When determining who is an authority, we have surprisingly low standards and respond instinctively. A blue uniform represents a policeman who should be obeyed, a white lab coat and stethoscope represents a doctor who's advice we should consider, and a man in a business suit must represent a respected business man who's opinions we should listen to. Cialdini (*)found three significant symbols of authority that will reliably trigger our compliance in the absence of the genuine substance of authority: titles, clothes, and trappings (jewelry, cars, etc.).	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
			(*)Cialdini, R. (1993), Influence: Science and practice (3rd edn), New York: HarperCollins	
Status	Social Biases	We act when our status seems in jeopardy, so be careful not to present status linked to undesired behaviour.	Provide feedback loops and measures that allow people to assess their standing and progress. Status relates to our standing relative to others or our personal best and can be both personal (income, performance, etc.) and public (scoring, recognition, etc.).	http://ui-patterns.com/patterns
Liking	Social Biases	We respond much more favorably to people and things we like and know than those we either do not like or are not familiar with. This fact can be used to increase the likelihood of strangers complying to your requests.	We tend to favor people with similar backgrounds and interests. Find a way to either assure your users that you are like them, or that your users are similar to them.	http://ui-patterns.com/patterns
Commitment & consistency	Social Biases	People like to be consistent with the things they have previously said or done. People generally want to be seen, as honoring their commitments consistently; as somebody who can be counted on, instead of somebody who flip flops, and is without self-control..	Find ways to make people state their agreement to a decision in order to pave way for similar and larger commitments in the same category, later.	http://ui-patterns.com/patterns
Reputation	Social Biases	We adjust our personal behaviour to reflect positively on how peers or the public perceive us.	Allow users to build reputation by contributing content, sharing information, connecting people, and performing activities that are in line with the purpose of your community.	http://ui-patterns.com/patterns

Design pattern	*Perspective*	*Explanation*	*Example*	*Source*
Role playing	Social Biases	People act according to their persona.	How we act depends on the social norms and constructs of a context we are in. Construct communities and contexts with norms allowing users to play a role their real-world persona would not allow.	http://ui-patterns.com/patterns
Reciprocation	Social Biases	We feel obliged to give when we receive.	Utilize the power of reciprocation by provoking or retaliating users to returning a favor or value provided for free.	http://ui-patterns.com/patterns
Revenge	Social Biases	If we feel we have been treated unfairly, we have an urge to want everyone else to know what that person did to us. Loss Aversion plays into this, as we perceive the value of a loss much greater than we do with gains and thus reciprocate more with anger than with joy.	Revenge can be encouraged to enforce positive and playful play; to beat friends in games or challenges.	http://ui-patterns.com/patterns
Social proof	Social Biases	We have a common tendency to adopt the opinions and follow the behaviours of the majority to feel safer and to avoid conflict.	Highlight certain behaviour to direct users' actions toward continuing that specific behaviour.	http://ui-patterns.com/patterns
Self-Expression	Social Biases	People seek opportunities to add a personal touch, resulting in deeper and longer engagements.	Find ways for users to express themselves. Allowing customization, posting content, commenting, following, sharing, and using emoticons are all ways that enable self-expression.	http://ui-patterns.com/patterns