Project Cyberstories

Text-mining- technieken voor de automatische herkenning van phishing mails

dr. Isa Maks, dr. Antske Fokkens, prof. dr. Piek Vossen

isa.maks@vu.nl, antske.fokkens@vu.nl, piek.vossen@vu.nl

Amsterdam, juli 2019

Computational Lexicology and Terminology Lab

Faculteit Geesteswetenschappen

Vrije Universiteit Amsterdam

vrije Universiteit amsterdam

Inhoudsopgave

Samenvatting

Dit verslag is gemaakt in het kader van het project *Cyberstories*. Het betreft het onderzoek naar de mogelijkheden van text mining technieken bij de automatische identificatie van frauduleuze mails. Er werd daarbij gebruik gemaakt van data beschikbaar gesteld is door de Fraudehelpdesk. We hebben de e-mails in deze databank bestudeerd en ons naar aanleiding daarvan verder gericht op een bepaald soort frauduleuze e-mails, nl. de phishing e-mails.

Een van de problemen is dat fraudeurs steeds beter worden. Niet alle fraudemails hebben spelfouten, niet alle mails worden van vreemd uitziende accounts verstuurd. Daar staat tegenover dat een aspect wel constant lijkt te zijn in phishing mails is het *gevoel van urgentie* dat wordt opgeroepen. Een oplichter wil graag dat iemand zo snel mogelijk en liefst zonder nadenken een (nep)rekening betaalt, op een link klikt om naar een valse website te gaan en daar inloggegevens en wachtwoorden in te vullen. Om dit gevoel van urgentie op te roepen, maakt de phisher - al dan niet bewust - gebruik van beïnvloedingstechnieken die beschreven worden binnen de gedragspsychologie.

In ons onderzoek combineren we de inzichten omtrent deze beïnvloedingsmethodes met text-mining-technieken en geven aan hoe dit ingezet zou kunnen worden bij de automatische identificatie van phishing e-mails. We hebben een lijst van *urgency cues* opgesteld en laten zien dat deze cues inderdaad gemiddeld meer in frauduleuze dan niet-frauduleuze e-mails voorkomen.

Ons onderzoek werd wel belemmerd door het feit dat we niet konden beschikken over een adequate dataset met phishing en niet-phishing e-mails nodig voor het ontwikkelen en testen van anti-phishing tools. We sluiten dan ook af met met een aantal aanbevelingen hoe een dergelijk dataset eruit moet zien.

1 Inleiding

Phishing mails en andere nepmails zijn een vorm van internetfraude. Hun doel is mensen naar valse websites te lokken en ze daar bijvoorbeeld te laten inloggen met hun wachtnaam en paswoord. Vervolgens gebruikt een fraudeur deze persoonsgegevens om geld af te schrijven van een bankrekening. Een ander soort nepmail is een spookfactuur waarbij iemand dringend verzocht wordt een -niet bestaande- achterstallige rekening te betalen.

In 2014 is de Fraudehelpdesk Nederland opgericht met als missie "burgers en bedrijven te behoeden voor oplichtingspraktijken en weerbaarder te maken tegen fraude.[1] Mensen die een nepmail denken te hebben gekregen kunnen die naar het meldpunt sturen. De mails worden verzameld in een database die de fraudehelpdesk helpt inzicht te krijgen in recente frauduleuze mails. Bovendien wordt de database doorzoekbaar gemaakt voor het publiek. Op dit moment kan de fraudehelpdesk niet van iedere mail zeggen frauduleus is of niet . Men schat (fraudehelpdesk, persoonlijke communicatie) dat ongeveer 20% van de mails in de database eigenlijk wel betrouwbaar is. Wij hebben de beschikking gekregen over een groot aantal van deze mails[2] met als doel te onderzoeken in hoeverre textmining technieken een bijdrage kunnen leveren aan de automatische herkenning van nepmails.

In dit rapport wordt eerst een beschrijving gegeven van bestaande benaderingen voor de automatische herkenning van frauduleuze mails (paragraaf 2). In paragraaf 3 gaan we in op de dataset met fraudemails die we voor dit onderzoek ter beschikking hebben gekregen. Vervolgens geven we aan hoe text-mining-technieken een bijdrage kunnen leveren aan de automatische herkenning van phishing mails (zie paragraaf 4.1). We sluiten we af met een conclusie en en aanbevelingen voor toekomstig onderzoek (zie paragraaf 5) .

[1] `https://www.fraudehelpdesk.nl`

[2] De betreffende e-mails zijn via een beveiligde verbinding ter beschikking gesteld en de VUA-onderzoekers hebben een verklaring ondertekend waarin zij toezeggen de mails alleen te gebruiken in het kader van het huidige project en de mails zelf of eventuele persoonsgegevens niet te delen met derden

2 Gerelateerd werk

Technische benaderingen om phishing attacks tegen te gaan detecteren op automatische wijze fraudulente emails en zorgen dat ze in iemands spambox terecht komen. Er worden verschillende methodes toegepast (zie ook [Chanti and Chithralekha, 2019]). Sommige van deze technieken zijn rule-based zoals bijvoorbeeld de "zwarte lijst¨methode.

1 Zwarte lijst: het aanleggen van zwarte lijsten met het email-adres van de afzender of domeinnaam van een frauduleuze afzender. Ook worden zwarte lijsten aangelegd met 'foute links' zodat emails die deze links bevatten niet bij een gebruiker terecht komen. Op zich werkt deze methode goed, maar niet in het geval van een 'zero day attack' waarbij het gaat om een nieuwe zending phishing mails die maar een paar uur duren en waarvan de gegevens nog niet op de zwarte lijst staan (zie [James et al., 2013]

De meeste methodes gebruiken echter machine-learning-technieken die zich bij de classificatie richten op de volgende eigenschappen van frauduleuze mails.

2 Automatische detectie van nep-URLS en nep-afzenders. Hierbij worden verdachte elementen in de structuur van de domeinnaam van de afzender en/of de URLs van de links gedetecteerd. ([Khonji et al., 2012, James et al., 2013]

3 Automatische detectie van nep-websites. Deze benadering detecteert of de website waar de links in de mail naar verwijzen betrouwbaar zijn. Er wordt dan gelet op de lay-out van de website en op het soort informatie dat gevraagd wordt, bijvoorbeeld of er gebruikersnamen en wachtwoord opgegeven moeten worden (zie [Leng Chiew et al., 2018]).

4 Structurele aspecten van de email. Er wordt een overzicht gemaakt van allerlei aspecten van de structuur van de mail: zijn er links naar andere websites en hoeveel, zijn er bijlages, bevat de email javascript en html, begint de e-mail met een aanhef en is deze persoonlijk of niet (zie [Rawal et al., 2017]).

5 Visuele aspecten: bij deze aanpak wordt gekeken naar het gebruik van logo's en naar de layout van de email en of die afwijken van niet-frauduleuze mails van de 'echte' afzender. ([Dunlop et al., 2010])

6 Aspecten die met het taalgebruik en de inhoud van de e-mail te maken hebben, zoals bijvoorbeeld of de teksten veel spelling- en grammaticale fouten bevatten. Ook wordt er gekeken naar de aanwezigheid van woorden als *paypay, bank account* en *click here*. Het idee is dat bepaalde woorden en concepten meer voorkomen in phishing dan in niet-phishing e-mails [Rawal et al., 2017]. Hierbij worden machine-learning technieken ingezet die onder meer gebruik maken van WordNet features ([Yasin and Abuhasan, 2016] en word vectors ([Moradpoor et al., 2017].

Over het algemeen worden Machine-learning-technieken toegepast met een combinatie van bovenstaande kenmerken ([Moradpoor et al., 2017], [Baykara and Gürel, 2018], [Rawal et al., 2017]), omdat een hybride aanpak tot de beste resultaten leidt (zie [Hajgude and Ragha, 2012]). Een voorwaarde is wel dat er datasets beschikbaar zijn met frauduleuze en niet-frauduleuze mails die gebruikt worden voor het trainen en testen van dit soort systemen. Voor het Engels zijn enkele van deze sets beschikbaar (zie [Leng Chiew et al., 2018], maar voor zover wij weten is dat voor het Nederlands niet het geval.

Het lastige is dat de tactieken van fraudeurs voortdurend veranderen. Zo is er volgens de laatste editie van Symantecs jaarrapport ([Symanantec, 2018]) op dit moment meer sprake van *spearphising* dan gewoon *phishing*. Terwijl bij *phishing* een grote hoeveelheid e-mails gestuurd naar veel mensen in de hoop dat iemand 'bijt', is *Spear phishing* persoonlijker gericht. Daarbij worden eerst gegevens over iemand verzameld (zoals naam, rekeningnummer en adres) en deze worden verwerkt in de valse mail. Mensen zijn dan geneigd toe te happen, omdat de e-mail betrouwbaar lijkt doordat er zoveel juiste informatie in staat. Bestaande anti-phising-methodes gaan er echter vanuit dat phishing mails niet met een persoonlijk aanhef beginnen en werken daardoor minder goed. Een ander voorbeeld ius dat er steeds meer gebruik gemaakt wordt van *spoofing* waarbij een e-mail verzonden wordt vanaf een (gehackt) bestaand mailadres. In deze gevallen falen bestaande anti-phising-methodes die gebruik maken van het feit dat URLs in frauduleuze mails verdachte elementen bevatten.

Niet alleen in het domein van de artificiële intelligentie wordt onderzoek gedaan naar phishing mails, maar ook binnen de gedragspsychologie. De vragen die daar gesteld worden gaan over de psychologische mechanismen die maken dat mensen slachtoffer worden van phishing. Uit dit onderzoek blijkt dat fraudeurs bepaalde beïnvloedingstechnieken gebruikt worden ([Ferreira et al., 2015]) en dat mensen geneigd zijn te reageren op zogenaamde *urgency cues* die in ruime mate aanwezig zijn in frauduleuze mails. Dit zijn woorden en zinnen die een gevoel van urgentie en zelfs dreiging oproepen en daarmee voorkomen dat iemand nog eens rustig nadenkt voordat hij klikt of "bijt"([Vishwanath et al., 2011].

Wij hebben onderzocht of de aanwezigheid van deze beïnvloedingstechnieken en bijbehorende *urgency cues* ook kan helpen bij de automatische detectie van phishing mails. Dat lijkt een interessante benadering te zijn juist omdat deze beïnvloedingstechnieken een constante factor zijn in frauduleuze mails waardoor de methode mogelijk beter bestand is tegen de voordurende wisselende tactieken van fraudeurs dan bestaande methodes. In paragraaf 4 gaan we daar verder op in.

3 Datasets

We hebbn gebruik gemaakt van de volgende datasets:

- een set e-mails van de Fraudehelpdesk met verdachte e-mails (zie paragraaf 3.1)
- een set van e-mails verzonden door financiële instellingen die naar alle waarschijnlijkheid niet frauduleus zijn (zie paragraaf 3.2)

3.1 Phishing e-mails van de Fraudehelpdesk

De set met frauduleuze e-mails is afkomstig uit het bestand van de Fraudehelpdesk. Deze helpdesk ontvangt en verwerkt ca. 80.000 verdachte e-mails per maand[3]. De mails worden opgeslagen in een database en een deel van de mails worden geanonimiseerd en op een demo-website gepubliceerd.[4]

Frauduleuze mails zijn op verschillende manieren in te delen: je kan kijken naar de afzender (is de mail gezonden namens een officiële instelling of namens een privépersoon), naar het doel (is de e-mail bedoeld om iemand op een link te laten klikken en naar een website te lokken of eerder om iemand direct geld te laten overmaken), naar de toon (valt er iets te winnen of wordt je kaart geblokkeerd en moet je boetes betalen). In alle gevallen is de inhoud van de mail niet waar. Er bestaan geen betaalachterstanden, superprijzen, verouderde betaalpassen, of afpersingsvideo's en de bedoelingen achter de e-mail zijn crimineel.

De database van de Fraudehelpdesk bevat e-mails die door leken (particulieren en ondernemers) zijn aangemerkt als verdacht en doorgestuurd naar de Fraudehelpdesk. De helpdesk schat dat 80% van deze e-mails frauduleus zijn, maar beoordeelt niet per e-mail of dit daadwerkelijk zo is. Alle e-mails worden opgeslagen in een databank voor nader onderzoek. Het grootste deel van de e-mails wordt zonder verdere bewerking opgeslagen in de databank, maar een klein deel wordt handmatig opgeschoond, geanonimiseerd en op de website gepubliceerd. Deze laatste worden ingedeeld in categorieën waarvan we hier een aantal belangrijke noemen.

- phishing mails: een phishing email richt zich op het verkrijgen van vertrouwelijke door mensen te lokken naar een valse website waar men dan (niets vermoedend) inlognaam, wachtwoord, creditcardnummer e.d. invult. Over het algemeen worden deze mails verstuurd zogenaamd namens een bank, creditcard bedrijf, belastingdienst of een andere officiële instelling verzonden en vragen mensen om op links of bijlages te klikken, gegevens in te vullen of geld over te maken (zie voor een voorbeeld, Appendix A: phishing mail).
- nep winmails: ook deze e-mails proberen iemand op een valse website te laten inloggen. Ze worden over het algemeen namens een winkel of een loterij gestuurd en stellen een mooie prijs in het vooruitzicht. Uiteindelijk wordt ook via deze mails 'gevist' naar persoonsgegevens of geld (zie voor een voorbeeld, Appendix A: valse winactie).
- spookfacturen: spookfacturen worden ook namnes officiele instellingen verzonden en zijn een factuur voor goederen of diensten die nooit geleverd geleverd zijn. Vaak gaat het bij spookfacturen om kleinere bedragen, omdat men daarbij sneller geneigd is te betalen en minder streng controleert.(zie voor een voorbeeld, Appendix A: spookfactuur)

[3] De dienstverlening is stopgezet per juli 2019, zie `https://www.fraudehelpdesk.nl/aanpassing-dienstverlening-valse-e-mails/`

[4] `https://www.fraudehelpdesk.nl/false_email_tag/valse-email/`

- afpersingsmails: afpersingsmails worden over het algemeen namens een particulier gestuurd. Er staat in dat je computer gehackt is na het bezoek aan een pornowebsite en dat je een bedrag moet betalen om te voorkomen dat gevoelige priv-informatie verspreid wordt. (zie voor een voorbeeld, Appendix A: afpersmail)

In het kader van het huidige onderzoek richten we ons alleen op de eerste categorie, die van de phishing mails die door een officiële - in dit geval financiële - instelling verzonden zijn. De belangrijkste reden hiervoor is dat we deze betrekkelijk makkelijk kunnen onderscheiden van de andere categorieën door te selecteren op de - vermeende - afzender.

Tabel 3.1 geeft een overzicht van de e-mails die we geselecteerd hebben. De set bestaat uit 2632 e-mails en is is opgedeeld in een set voor evaluatie (test set) en een test voor ontwikkeling (development set).

Tabel 1: Set phishing e-mails gebruikt in dit onderzoek

Vermeende afzender	**Test set**	**Development set**
ING (ING-bank)	327	36
CJIB (Centraal Justitieel Incassobureau)	541	70
RABO (RABO-bank)	419	45
ABN (ABN-bank)	397	41
ICS (International Creditcard Services)	675	92
totaal	2359	284

3.2 Niet-phishing e-mails

Naast de set met phishing mails hebben we ook een set met 'echte' niet-phishing mails verzameld. De bedoeling was dat deze wat betreft afzender, vorm en inhoud zoveel mogelijk lijken op de verzamelde phishing mails. We hebben banken benaderd en geprobeerd de beschikking te krijgen over een set e-mails die zij in de afgelopen periode verzonden hebben naar hun klanten. Helaas is dit niet gelukt en hebben we onze strategie moeten wijzigen.

De uiteindelijke set non-phishing mails bestaat uit 54 e-mails gestuurd aan één persoon en door die persoon verzameld. De mails zijn verstuurd door banken en betreffen allerlei financiële handelingen zoals het openen het afsluiten van rekeningen, het afsluiten van hypotheken en het betalen servicekosten.

Tabel 2: Set non-phishing e-mails gebruikt in dit onderzoek

Afzender	**Test set**
Aegon bank en verzekeringen	15
ASN	11
Knab bank	9
RABO	9
Triodos	7
overig	3
totaal	54

De e-mails zijn qua inhoud en vorm geschikt voor dit onderzoek aangezien ze goed passen bij de set van phishing e-mails die we verzameld hebben, maar de set heeft ook een aantal tekortkomingen. Om te beginnen is ook deze set niet verzameld door een expert op het gebied van fraudedetectie wat betekent dat er e-mails tussen kunnen zitten die wel frauduleus zijn. Daarbij is de set in ieder geval te klein om in te kunnen zetten als trainingset bij een machine-learning-benadering, maar hij is ook eigenlijk aan de kleine kant om in te zetten als evaluatieset.

4 Expressies van urgentie voor automatische herkenning van phishing mails

In het kader van het huidig onderzoek hebben we bekeken in hoeverre text-mining-technieken een bijdrage kunnen leveren aan de automatische idenficatie van phishing e-mails. We hebben ons hierbij gericht op het 'gevoel van urgentie' dat door veel phishing e-mails wordt opgewekt en dat door phishers al dan niet bewust wordt ingezet om mensen snel te laten reageren.

4.1 Het gevoel van urgentie in phishing e-mails

Phishing mails lijken erg op e-mails van betrouwbare instanties zoals banken, bekende webshops of de overheid. Dezelfde opmaak, niet of nauwelijks spelfouten en met links die niet makkelijk te onderscheiden zijn van originele links. Dit wekt vertrouwen bij de ontvanger van het bericht, waardoor de mail eerder geopend wordt en de ontvanger sneller op hyperlinks in het bericht klikt. Uit onderzoek blijkt echter dat in phishing mails meer dan in gewone mails een 'gevoel van urgentie' gecreëerd wordt waardoor de ontvanger snel reageert en op een (malafide) hyperlink klikt. Daarbij worden beïnvloedingstechnieken zoals bekend uit de gedragspsychologie gebruikt ([Lastdrager, 2018], [Ferreira et al., 2015]).

Phishers gebruiken 'cues voor urgentie' om angst, dreiging en een idee van schaarste over te brengen. Mensen focussen op deze cues en missen daardoor andere verdachte kenmerken van de email (zoals een verdachte afzender, of een ongewoon uitziende hyperlink) [Vishwanath et al., 2011]. De speciale strategieën die gebruikt worden om het gevoel van urgentie op te roepen, worden ook in de marketing gebruikt en bevatten onder andere de volgende elementen: [5]

- *Create a sense of scarsity* Als een product zeldzaam is of zeldzaam wordt, dan lijkt het meer waard. Door de schaarste van het product of dienst te benadrukken, krijgt iemand het gevoel snel te moeten handelen.
  Bijvoorbeeld: *OP=OP, Er zijn er nog 3 beschikbaar*

- *Call to action* Geef duidelijk aan wat iemand moet doen.
  Bijvoorbeeld: *Download en installeer de ING antivirus meteen, Nu beveiligen , U kunt nu onmiddelijk uw schuld voldoen op het hieronder genoteerde rekeningnummer, U dient uw Mijn ING binnen 2 dagen na ontvangst van deze mail te updaten.*

- *Introduce an unpleasant situation* Vertel iemand dat hij in een vervelende situatie verzeild is geraakt en een probleem heeft. Hij of zij wordt onrustig en reageert meteen zodat het probleem snel wordt opgelost.
  Bijvoorbeeld: *Er is geprobeerd een online betaling te verrichten met uw card, U maakt nog gebruik van een verouderde pas*

- *Framing of loss* Vertel iemand wat hij heeft te verliezen als hij geen actie onderneemt. Als iemand het gevoel krijgt dat er iets ërgs' gebeurt (rekening wordt geblokkeerd) dan zal hij geneigd zijn snel tot actie over te gaan. Dit veroorzaakt een lichte angst, en kan ook zelfs in de vorm van een dreigement gebracht worden [Williams et al., 2017].
  Bijvoorbeeld: *Om te voorkomen dat uw toegang tot de app wordt geweigerd, Het OM zal de politie opdracht geven om te signaleren en u in gijzeling te nemen voor 7 dagen*

[5] https://marketingland.com/12-ways-use-urgency-psychology-improve-conversions-112603

- *Framing of gain* Vertel iemand wat hij heeft te winnen als hij wel actie onderneemt. Ook dat zal inhouden dat hij of zij snel tot actie overgaat , zodat hij of zij niet het risico loopt het beloofde voordeel mis te lopen.
  Bijvoorbeeld: *Wij zullen dan alle blokkades opheffen, U komt in aanmerking voor een belasting-teruggave*

- *Set a Deadline* Geef een deadline waarna het niet meer mogelijk is om te reageren.
  Bijvoorbeeld: *Als u de update niet binnen twee weken installeert, Uw betaling dient voor 11-04-2018 bij ons binnen te zijn.*

- *Use time-sensitive language* Door te verwijzen naar het feit dat de tijd een rol speelt en voorbijgaat, wordt het gevoel van urgentie en de noodzaak om tijdig handelen nog verder vergroot.
  Bijvoorbeeld: *Het verifiëren van uw rekening duurt ongeveer 5 minuten, U ontvangt de Rabopas binnen enkele werkdagen per post*

We hebben een set van 284 phishing mails (zie Tabel 3.1: development set) geanalyseerd en bekeken in hoeverre bovenstaande technieken daadwerkelijk gebruikt worden. Hieronder is een voorbeeld te zien (Figuur 3).

Opvallend is dat niet alle soorten expressies voorkomen: expressies van schaarste hebben we niet kunnen vinden. Sommige expressies zoals *verlopen* kunnen zowel als 'framing of loss' gezien worden als als een 'time-sensitive language'. In dit geval hebben we voor de laatste gekozen, maar het geeft aan dat de anotaties ook wel; ambigu kunnen zijn. In onderstaande e-mail komen ook geen verwijzingen naar een vervelende situatie (Unpleasant situation) voor. Dat lijkt toeval te zijn, want in de andere mails hebben we deze wel gevonden (zie Appendix B voor een overzicht).

Tabel 3: Een voorbeeld van een phishing mail met annotaties voor expressies van urgentie

Toelichting:
Reference to scarcity
Call to action
Unpleasant situation
Framing of loss
Framing of gain
Setting a deadline
Use time-sensitive language

From: De Rabobank
Sent: Thursday, April 12, 2018 6:51 AM .
To:
Subject: Uw pas verloopt bijna .

bankpas verloopt bijna .
U ontvangt dit automatische bericht omdat uw bankpas binnenkort verloopt . In deze e-mail leggen wij uit hoe u direct een nieuwe bankpas aanvraagt . U kunt tot 12 april 2018 uw bankpas kosteloos vervangen . Daarna betaalt u hier eenmalig €14,95 voor

Nieuwe bankpas aanvragen
U vraagt uw nieuwe bankpas kosteloos aan via uw unieke link [rabobank.nl/ aanvragen.]
Houd uw Rabo Scanner bij de hand en log in zoals u dat normaal ook doet. Uit veiligheidsoverwegingen vragen wij u om een aantal persoonsgegevens.

U ontvangt uw nieuwe bankpas binnen 5 werkdagen . Indien u een nieuwe pincode heeft gekozen, ontvangt u hier schriftelijk bevestiging over.
Let op: tot 14 april 2018 kunt u de bankpas kosteloos aanvragen . Daarna betaalt u hier €14,95 voor.

Nog vragen?
Heeft u nog vragen over het aanvragen van uw nieuwe bankpas? Neem dan contact op met onze klantenservice. Onze klantenservice is op werkdagen bereikbaar van 8.00 tot 17.00 uur.
Met vriendelijke groet,
Afdeling Bankzaken
Rabobank
Dit is een automatisch verstuurd bericht van Rabobank. Indien deze e-mail niet voor u is bedoeld, kunt u deze negeren.

4.2 Distributie van expressies van urgentie in phishing versus non-phishing mails

De volgende stap in ons onderzoek bestond uit het tellen van dit soort expressies in phishing en niet-phishing om te zien of de veronderstelling klopt dat urgentie eerder wordt opgeroepen in phishing dan in niet-phishing mails. Aangezien het om een eerste verkennend onderzoek gaat, hebben we alleen gekeken naar expressies die bestaan uit één woord ('klikken', 'meteen') en meer-woord-expressies die uit een vaste opeenvolging van woorden bestaan ('op tijd', 'geen toegang meer', 'betere beveiliging'). Dat houdt dus in dat langere expressies zoals 'dat leidt tot vervelende consequenties' (Loss) in deze analyse niet worden meegenomen.

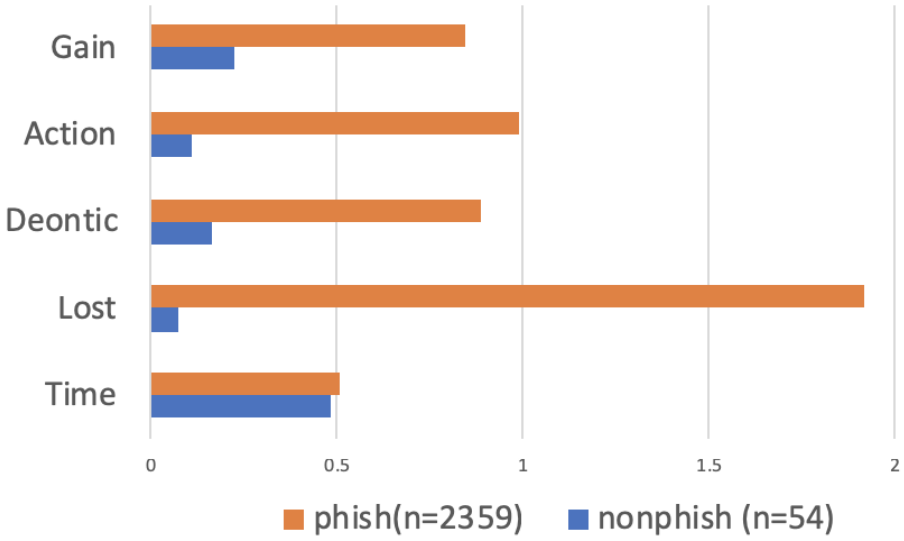
In Tabel 4 worden per urgentie-categorie de woorden ('urgency cues') gegeven die we geteld hebben in de mails. Een aantal categorieën hebben we samengevoegd, omdat zij moeilijk uit elkaar te halen waren als alleen naar woorden zonder contekst gekeken wordt. Zo zijn 'Time-sensitive language'en 'Setting a deadline' samengevoegd tot één categorie Time. Ook 'Framing of loss' ('om te voorkomen dat u geen toegang meer heeft tot uw mobiel bankieren app') en 'Unpleasant situation' ('u heeft op dit moment geen toegang meer tot mobiel bankieren') zijn samengevoegd tot één categorie Loss. 'Call to action', daarentegen, is gesplist in twee categorieën: Action en Deontic. Action bevat woorden die specifieke acties beschrijven (zoals 'klikken', 'aanvragen', 'betalen'), terwijl 'Deontic modality (Deontic) woorden die meer in het algemeen aangeven dat iets noodzakelijk of verplicht is (zoals 'moeten' en 'dienen').

Tabel 4: *Urgency cues* voor het meten van urgentie in tekst

Time	time-sensitive language putting a deadline	binnenkort, urgentie, meerdere malen, laatste, op tijd, eerder, gauw, dringend, meteen, onmiddellijk, snel, spoedig, terstond, zojuist, dadelijk, op dit moment , eenmalig, eenmalige
Action	call to action	hier, let op, heraanvraag, voorkomen, voorkom , voorkomt , klikken, klik , klikt, opsturen, direct betalen, verifieer, verifieert, verifieren, voldoen, voldoet, start
Deontic	call to action	moet, verplicht, dient, dienen, moeten, genoodzaakt
Loss	unpleasant situation framing of loss	vervelende consequenties, geen toegang meer, geen betalingsregeling meer, betalingsachterstand, aanmaning, ongelezen, opheffen, afgekeurd, geen geld meer, schuld, naheffing, gerechtsdeurwaarder, beslag , ongeldig, verlopen, vervalt, verval , schorsing, erger, verloopt, verouderd, nadelig, geblokkeerd , blokkade, blokkeren, blokkering, beperkt, gijzeling, verouderd
Gain	framing of gain	kosteloos, deblokkeren, vervangen, beter beveiligd, gratis, vernieuwd, verbeterd , toegang herstellen
Scarsity		n.v.t.

De resultaten van de 'meting' zijn in Figuur 1 te zien. Per urgentie-categorie zijn de cues geteld in zowel de 2359 phishing mails en de 54 non-phishing mails. Om de resultaten te kunnen vergelijken zijn gemiddelden berekend door het totaal aantal cues te delen door het aantal e-mails in de categorie 'phishing' danwel 'non-phishing'. We zien dat alle urgentie-categorieën rijker vertegenwoordigd zijn in

de phishing mails dan in de non-phishing mails. Het is wel zo dat het gemiddeld aantal tijdsexpressies(Time) in phishing en niet-phishing e-mails ongeveer even groot is, wat inhoudt dat die categorie maar in zeer beperkte mate een onderscheidende werking heeft.



Figuur 1: Gemiddeld aantal urgentie-expressies in phishing en niet-phishing e-mails
x-as : (aantal expressies / aantal e-mails)

4.3 Automatische herkenning van phishing e-mails

Aangemoedigd door de resultaten van de vorige paragraaf (zie Figuur 1), hebben we als laatste stap een simpel classificatie-algoritme gemaakt. Het algoritme telt woorden en maakt daarbij gebruik van de woorden van Tabel 4. In dit geval is het doel phishing mails van non-phishing mails te onderscheiden.

De evaluatieset bestaat uit 2359 phishing mails en 44 (van de totale set van 54) non-phising e-mails. De overige 10 non-phishing en 284 phishing e-mails zijn gebruikt voor de ontwikkeling van de classifier en met name om de drempel te bepalen stellen waarboven een e-mail als 'phishing' geclassificeerd wordt. Die drempelwaarde is vastgesteld op n≥1 wat inhoudt dat e-mails met geen enkele urgentie-expressie als 'niet-phishing' geclassificceerd worden en alle andere als 'phishing'.

De resultaten zijn te zien in Tabel 5. De classificatie is uitgevoerd met alle 5 categorieën urgentie-expressies (zie kolom I) en met alleen de categorieën Action, Deontic, Loss en Gain (zie kolom II). De prestaties van de classifier worden gegeven aan de hand van scores voor *precision* (hoeveel van de e-mails die door de classifier als phishing worden gezien zijn ook daadwerkelijk phishing e-mails en hoeveel van de e-mails die door de classifier als niet-phishing worden gezien zijn ook daadwerkelijk niet-phishing e-mails), *recall* (hoeveel van de phishing en niet-phishing e-mails worden correct gevonden) en F1-score (het harmonische gemiddelde tussen recall en precision).[6]

De scores laten zien dat de classifier beter is in het herkennen van phishing e-mails dan non-phishing e-mails (methode I: 0,97% vs. 0,32% en methode II: 0,97 vs. 0,27%). Sterker nog, deze classifier heeft een *bias* en classificeert het grootste deel van de e-mails als 'phishing' waardoor zowel precision als recall laag uitvallen voor de niet-phishing categorie. Ons vermoeden dat tijdsexpressies niet een goede indicatie voor phishing zijn wordt bevestigd met als we kijken naar de scores van methode I en II. We zien ook dat de F1-score voor non-phishing mails iets verbetert (van 0.23 naar 0.27) als de tijdsexpressies niet worden meegenomen.

Tabel 5: Resultaten van classificatie (precision(p), recall(r) en F1-score(f))

	I			II		
	p	r	f	p	r	f
phishing mails	0,99	0,96	0,97	0,99	0,95	0,97
non-phishing mails	0,15	0,43	0,23	0,17	0,57	0,27
gemiddelde			0,60			**0,62**

We moeten concluderen dat simpele algoritme dat we hier hebben toegepast niet goed werkt. Een reden kan zijn dat we - bij gebrek aan voldoende data - geen analyse hebben kunnen maken van de non-phishing e-mails. Als we bijvoorbeeld kijken naar onderstaand fragment dat afkomstig is uit een non-phishing mail dan zien we dat bepaalde tijdsuitdrukkingen ook veelvuldig gebruikt worden in non-phishing mails (zie Tabel 6: non-phishing). Een belangrijker reden is dat met een simpel algoritme als het tellen van woorden, de rol van contekst genegeerd wordt. Onderstaande fragmenten laten bijvoorbeeld zien hoe de contekst een zinnetje als *zo snel mogelijk* bijna in heel verschillend licht

[6] berekening van precision, recall en F1:
precision: TP/(TP+FP)
recall= TP/(TP+FN)
F1= (2*(precision*recall))/precision+recall
TP=true positives - FP=false positives - FN=false negatives

Tabel 6: Fragmenten uit e-mails

non-phishing	U heeft *kort geleden* een aanvraag gedaan om uw ASN Wereldpas uit te zetten voor gebruik buiten Europa. Wij verwerken uw aanvraag binnen **zo snel mogelijk**.
phishing	Klik hier om **zo snel mogelijk** uw account te bevestigen.

plaatst. In het geval van de non-phishing e-mail (zie Tabel 6: non-phishing) slaat *zo snel mogelijk* op iets dat de bank voor de cliënt gaat doen, waardoor het een vriendelijke bijklankt krijgt. In het geval van de phishing e-mail (zie Tabel 6: phishing) betreft het echter iets dat de cliënt zelf moet doen. Daarmee draagt de uitdrukking in hoge mate bij aan een gevoel van urgentie en krijgt bijna een dreigende betekenis.

Er zijn geavanceerde text-mining-technieken die rekening houden met contekst. Om die te kunnen gebruiken moeten we echter wel kunnen beschikken over grotere en meer gebalanceerde datasets dan nu het geval is. Uit het feit dat phishing e-mails over het algemeen wel meer expressies van urgentie bevatten dan non-phishing e-mails (zie Paragraaf 4.2), maken we op dat deze een belangrijke rol kunnen spelen bij de identificatie van phishing e-mails mits ze ingebed worden in meer geavanceerde text-mining-technieken.

5 Conclusie

Dit rapport beschrijft hoe text mining een bijdrage kan leveren aan de de automatische herkenning van frauduleuze e-mails. Er werd daarbij gebruik gemaakt van data beschikbaar gesteld is door de Fraudehelpdesk en we hebben ons vooral gericht op de identificatie van phishing e-mails. We hebben onderzocht of we het gevoel van urgentie dat wordt opgewekt in frauduleuze mails konden herkennen door te zoeken naar *urgency cues*.

Ons onderzoek wees uit dat deze cues inderdaad in verhouding meer voorkomen in phishing e-mails dan in non-phishing e-mails . Het interessante van de benadering is dat het gevoel van urgentie wordt opgeroepen in alle soorten frauduleuze e-mails een constante factor lijkt te zijn. Met fraudeurs die voortdurend van tactiek veranderen maar wel altijd willen dat de e-mail met urgentie afgehandeld moet worden, zou een methode die ook gebruik maakt van *urgency cues* wel eens robuuster kunnen zijn dan bestaande methodes.

Een belangrijke conclusie van ons onderzoek is dat als je serieus werk wilt maken van verdere ontwikkeling van anti-phishing tools voor het Nederlands, er een adequate dataset aangelegd moet worden die geschikt is voor het trainen en testen van de tools. De dataset moet van voldoende omvang zijn en bestaan uit twee subsets: een set frauduleuze e-mails en een set niet-frauduleuze e-mails. Het blijkt niet eenvoudig een dergelijke set samen te stellen. De e-mails die beschikbaar zijn bij de Fraudehelpdesk zijn zeer waardevol, maar volstaan niet. Bedrijven en instellingen zoals banken stellen niet zomaar de e-mails die zij aan klanten sturen ter beschikking. Daarnaast moeten de subsets ook op elkaar aansluiten in de zin dat als de set met frauduleuze e-mails spookfacturen bevat, de set met niet-frauduleuze e-mails ook facturen bevat. Hieronder volgt een aantal punten waarop gelet moet worden bij het samenstellen van een geschikte dataset.

Frauduleuze mails

- anonimisatie: de data moeten geanonimiseerd zijn zowel wat betreft de afzender als de geadresseerde. De e-mails die in de databank van de Fraudehelpdesk zitten bevatten namen, (e-mail-adressen) en soms bankgegevens van zowel de afzender als de geadresseerde. Het is niet triviaal om deze gegevens te verwijderen en het is de vraag of standaard-software in dit geval volstaat. Het belang van anonimisatie is vooral groot als de dataset ter beschikking gesteld wordt aan derden voor bijvoorbeeld de ontwikkeling van tools.

- betrouwbaarheid: de e-mails moeten gecontroleerd worden door een expert om zeker te weten of ze frauduleus zijn of niet. Het betrekkelijk grote aandeel van de dataset (20%) van niet-frauduleuze e-mails vormt een serieus probleem bij het betrouwbaar testen van automatische tools.

- categorisatie: de databank van de Fraudehelpdesk bevat veel verschillende soorten frauduleuze e-mails zoals nep winmail, spookfacturen, chantagemails, etc. Het zou goed zijn als een indeling gemaakt kon worden en de mails volgens deze indeling gelabeld zouden worden. De indeling die gehanteerd wordt door de Fraudehelpdesk bij het publiceren van demo-mails is een goede start, maar definities en criteria ontbreken.

- representativiteit en variatie: de e-mails moeten een afspiegeling zijn van de frauduleuze e-mails die in omloop zijn. De databank van de Fraudehelpdesk is up-to-date aangezien hij dagelijks

aangevuld en vermoedelijk ook voldoende representatief voor wat er is. Het is zaak ook voldoende variatie in de e-mails te hebben wat betreft soort frauduleuze e-mail. De categorisatie (zie vorig punt) vormt een belangrijk punt in het garanderen en .. van deze variatie.

Niet-frauduleuze mails

- anonimisatie: zie frauduleuze mails.
- betrouwbaarheid: Als e-mails worden aangeleverd door leken, moet door experts op het gebied van nepmails bekeken worden of het inderdaad een echte mail is. Dit kan ook opgelost te worden door samen te werken met de instellingen en de e-mails te verzamelen die zij versturen aan hun klanten.
- categorisatie: Net als bij de frauduleuze e-mails moeten ook de niet-frauduleuze mails ingedeeld zijn. Wie heeft ze verstuurd, wat is het onderwerp en doel van de e-mail. Alleen op die manier kan een goede set worden samengesteld die 'matcht' met een set van vergelijkare e-mails frauduleuze mails.

Referenties

[Baykara and Gürel, 2018] Baykara, M. and Gürel, Z. Z. (2018). Detection of phishing attacks. *Proceedings of Digital Forensic and Security (ISDFS)*.

[Chanti and Chithralekha, 2019] Chanti, S. and Chithralekha, T. (2019). Classification of anti-phishing solutions. *SN Computer Science*, 1(1):11.

[Dunlop et al., 2010] Dunlop, M., Groat, S., and Shelly, D. (2010). Goldphish: Using images for content-based phishing analysis. In *2010 Fifth International Conference on Internet Monitoring and Protection*, pages 123–128.

[Ferreira et al., 2015] Ferreira, A., Coventry, L., and Lenzini, G. (2015). Principles of persuasion in social engineering and their use in phishing. In *Proceedings of HAS-2015 (Human Aspects of Information Security, Privacy, and Trust)*.

[Hajgude and Ragha, 2012] Hajgude, J. and Ragha, L. R. (2012). "phish mail guard: Phishing mail detection technique by using textual and url analysis". *2012 World Congress on Information and Communication Technologies*, pages 297–302.

[James et al., 2013] James, J., L, S., and Thomas, C. (2013). Detection of phishing urls using machine learning techniques. pages 304–309.

[Khonji et al., 2012] Khonji, M., Iraqi, Y., and Jones, A. (2012). Enhancing phishing e-mail classifiers: A lexical url analysis approach. *International Journal for Information Security Research*, 2:236–245.

[Lastdrager, 2018] Lastdrager, E. (2018). *From fishing to phishing*. PhD-thesis, University of Twente.

[Leng Chiew et al., 2018] Leng Chiew, K., Hung Chang, E., Tan, C. L., Abdullah, J., and Yong, K. (2018). Building standard offline anti-phishing dataset for benchmarking. *International Journal of Engineering Technology, 7 (4.31) (2018) 7-14International Journal of Engineering Technology*, pages 7–14.

[Moradpoor et al., 2017] Moradpoor, N., Clavie, B., and Buchanan, B. (2017). Employing machine learning techniques for detection and classification of phishing emails. *2017 Computing Conference*, pages 149–156.

[Rawal et al., 2017] Rawal, S., abd Aakhila Shaheen, B. R., and Malik, S. (2017). Phishing detection in e-mails using machine learning. *International Journal of Applied Information Systems*, 12.

[Symanantec, 2018] Symanantec (2018). Internet security threat report. 23.

[Vishwanath et al., 2011] Vishwanath, A., Herath, T., Chen, R., Wang, J., and Rao, H. R. (2011). Why do people get phished? testing individual differences in phishing vulnerability within an integrated, information processing model. *Decision Support Systems*, 51(3):576 – 586.

[Williams et al., 2017] Williams, E. J., Morgan, P. L., and Joinson, A. N. (2017). Press accept to update now: Individual differences in susceptibility to malevolent interruptions. *Decision Support Systems*, 96:119 – 129.

[Yasin and Abuhasan, 2016] Yasin, A. and Abuhasan, A. (2016). An intelligent classification model for phishing email detection. *CoRR*, abs/1608.02196.

A Appendix: Voorbeelden van verschillende soorten fraudemails

Phishing mail

Geachte heer/mevrouw,
Als klant wilt u duidelijk en tijdig genformeerd worden over veranderingen van onze producten en diensten. Wij brengen u graag op de hoogte van nieuwe ontwikkelingen.
Wat gaat er nu gebeuren? ABN AMRO wilt u graag de nieuwe betaalpas introduceren. Wij hebben de laatste tijd veel last van storingen en misbruik van betaalpassen, om dit te stoppen hebben wij een nieuwe omgeving ontwikkeld die hier tegen gewapend is.
Op dit moment maakt u nog geen gebruik van onze nieuwe omgeving. Wij betreuren dit omdat u nu niet volop van ons systeem gebruik kunt maken. Nadat u uw nieuwe betaalpas heeft ontvangen wordt automatisch de nieuwe ABN AMRO Internet Bankieren omgeving geconfigureerd.
Introductie nieuwe ABN AMRO betaalpas Om de nieuwe betaalpas in ontvangst te kunnen nemen moet u eerst het formulier invullen. U kunt via de onderstaande link de aanvraag voltooien.
Nieuwe betaalpas aanvragen
Vragen en meer informatie Heeft u een vraag? Bel met n van onze medewerkers, via (gebruikelijke belkosten). Dat kan 24 uur per dag, 7 dagen per week.
Met vriendelijke groet, ABN AMRO Bank N.V.

Valse winactie

Beste
Goed nieuws! Het weer tijd voor een ****** winactie Dit keer geven wij een Blokker waardebon t.w.v. 500,- weg!
Mogelijke winnaar: Controleer snel of jij er deze week met de prijs vandoor gaat.
Meedoen duurt 2 minuten en kost niets. 1. Vul jouw gegevens in 2. Beantwoord de enqute 3. Bekijk jouw prijs Nu meedoen ¿
DOE NU MEE!
Als u deze aanbieding niet leuk vindt, klik dan hier om u af te melden. Uitschrijven kan via deze link

Spookfactuur

Subject: Beslag op uw bankrekeningen, voorkom nu! Laatste kans!
PERSOONLIJK VERTROUWELIJK!
U heeft meegedaan een enquete waarbij u een cadeaukaart kon winnen, u bent akkoord gegaan met de algemene voorwaarden (artikel 11.9.2; Er zijn kosten van EUR 0.99 verbonden aan deelname) en op grond van deze voorwaarden incasseren wij nu de vordering. Onze gerechtsdeurwaarder zal vandaag bij u langskomen voor het leggen van beslag, tenzij u direct de vordering voldoet. Gegevens dossier:
Dossiernummer: **
Ons kenmerk: **
Openstaand bedrag: EUR 101.71
De kosten van de dagvaarding, het beslag en de gerechtelijke griffiekosten zijn begroot op EUR 805.40, wanneer u niet direct de vordering voldoet zullen we u deze kosten extra in rekening brengen.
Als u deze extra kosten en het beslag wilt voorkomen dient u direct de openstaande som te voldoen aan ons kantoor tegen finale kwijting.
Voorkom beslag op uw inkomen, bankrekeningen en inboedel en betaal direct de openstaande EUR 101.71!
Onze bankgegevens:
IBAN: DE***
Ten name van: Derdengelden gerechtsdeurwaarders
Omschrijving: ** Bedrag: 101.71 euro
Neem onze bankgegevens exact over om te voorkomen dat uw betaling verkeerd loopt, bij betaling aan andere gegevens dan deze gegevens kunnen we het beslag en de extra kosten niet voorkomen!
Betaal direct en voorkom beslag op uw inboedel, bankrekeningen en uw inkomen.
Onder voorbehoud van alle rechten en weren,
Hoogachtend,
Afdeling incasso, debiteuren
Incasso-jurist

Afpersmail

From: NU Lesen!!! .
*Sent:** Friday, February 1, 2019 10:05 AM .
*Subject:** SNELPOST .
*Beste,** .
*Mijn naam is Arnold, dat is teminste hoe ze me noemen op de deepweb redrooms. Ik heb deze mailbox meer dan zes maanden geleden gehackt, Sindsdien heb ik je besturingssysteem geinfecteerd met een virus (trojan) dat door mij is gemaakt en heb ik je lange tijd gevolgd. Zelfs als je het wachtwoord daarna hebt gewijzigd het maakt niet uit, mijn virus heeft alle cachegegevens van uw computer onderschept en geeft mij automatisch opnieuw toegang.
Ik heb toegang tot al uw accounts, sociale netwerken, e-mail, browsegeschiedenis. Dienovereenkomstig heb ik de gegevens van al uw contacten van u mobiel, bestanden van uw computer, fotos en videos alles maar ook echt alles. Ik was het meest in de lach geschoten door de intieme inhoudssites die je af en toe bezoekt. Je hebt een heel wilde fantasie, ik zeg het je AHHAHAH! Tijdens je tijdverdrijf en entertainment daar, nam ik een screenshot via de camera van al je apparaten die ik maar kon bereiken, en verstuurd naar mij. O mijn God! Je bent zo grappig en opgewonden! Ik kan nu al niet wachten tot ik je deze email zie lezen HAHA Ik denk dat je niet wilt dat al je contacten deze bestanden krijgen, toch? Als je van dezelfde mening bent, dan denk ik dat 50 euro een vrij redelijke prijs is om het vuil te vernietigen.
*Stuur het bedrag maar naar mijn BTC-portemonnee (bitcoin): _13yeuff897dzMkRqTS oEpG4TLyHeAZ1nf4**
*Zodra het bovenstaande bedrag is ontvangen, garandeer ik dat de gegevens worden verwijderd, ik heb het niet nodig. Op deze manier heb ik en behoud ik zolang nodig ook toegang tot al je accounts, social network, contacten, emails, browsing geschiedenis, etc. Alle data die bruikbaar is, zowel contacten als gegevens als fotos en videos zijn zorgvuldig opgeslagen. De sexuele interesses die jij koestert, de sites die jij bezoekt, zijn op zijn zachts gezegd interessant te noemen. Tijdens deze handelingen gedurende tijd, heb ik screenshots via jouw camera gemaakt, die synchroom lopen met wat jij aan het kijken bent. Als je niet wilt dat ik deze gegevens en interesses deel met familie, vrienden, kennissen, collegas en omgeving; Betaal dan 50 euro. Dit bedrag is zeer schappelijk, vergeleken met de schade die ik kan aanrichten.
U kunt betalen d.m.v. een Crypto Voucher. 50 euro Crypto Voucher:
Crypto Voucher: [**https:// igiftcards.nl/cryptovoucher/ giftcard?v=50 c=eur**] (https://igiftcards.nl/ cryptovoucher/giftcard?v=50 c=eur)
Stuur de code die u na betaling ontvangt naar:
rabospar@mail.com
Zodra de code is ontvangen, garandeer ik dat alle data verwijderd zal worden, ik heb het niet nodig. Indien je niet betaald, zal ik er geen seconde over twijfelen daad bij woord te voegen. Vanaf het moment van openen van deze e-mail geef ik je 24 uur de tijd om te betalen. Ik ontvang automatische een notificatie wanneer je deze e-mail hebt geopend. Vanaf dan begint de tijd te lopen.
Sterkte.”,t

B Appendix: Voorbeelden van expressies van urgentie in phishing mails

Tabel 7: Voorbeelden

Urgency category	**Text**
Action Gain Time	Verifieer uw rekening eenmalig om blokkade te voorkomen
Action Gain	U kunt dit nog voorkomen om het openstaande bedrag van **247,80** te voldoen op rekeningnummer **LT403510000019626 81**
Action Time	**Let op:** download en installeer de ING antivirus meteen.
Action Time	Nu beveiligen ¡http://w¿
Action Time	Indien u niet onmiddelijk uw schuld voldoet op het hieronder genoteerde rekeningnummer,
Action Time	Let op: u dient uw Mijn ING binnen ontvangst van deze mail te updaten.
Action Time	U bent verplicht jaarlijks uw apparaat of toestel opnieuw te registreren of te verlengen
Action	[Vernieuwde Rabopas aanvragen](http://x.co/3904fjke)
Action	Om u Card en Mijn ICS weer te kunnen gebruiken moet u uw gegevens verifiren.
Action	U dient op de gegeven link te klikken om deze verificatie te starten
Action	Verificatie uitvoeren
Deadline	Als u de update niet binnen twee weken installeert
Deadline	Uw betaling dient voor 11-04-2018 bij ons binnen te zijn.
Gain Action	Wij vragen u om een eenmalige verificatie te doen om blokkade van uw rekening te vermijden.
Gain Deadline	U heeft tot en met 20 december 2018 de gelegenheid om zonder kosten de vernieuwde Rabopas aan te vragen.
Gain	De app is compleet vernieuwd en gunstig voor de consumenten van ING.
Gain	Met deze verificatie kunnen wij uw rekening actief houden,
Gain	Als uw gegevens correct zijn geverifierd zullen wij alle blokkades opheffen.
Gain	hebben we vastgesteld dat u in aanmerking komt voor een belastingteruggave
Gain	om weer volledig gebruik te kunnen maken van alle diensten die ICS verleent.
Loss Time	Wij willen u erop attenderen dat financile schade door middel van frauduleuze activiteiten niet is verzekerd bij toekomstig gebruik van uw verouderde Rabopas.

Continued on next page

Tabel 7 – continued from previous page

Urgency category	Text
Loss	zullen we uw online bankieren tijdelijk uitschakelen als beveiligingsmaatregel.
Loss	U dient dan rekening te houden met nadelige gevolgen.
Loss Action Deadline	anders zijn wij genoodzaakt om uw rekening te blokkeren tot u deze verificatie heeft gedaan.
Loss	Anders word uw rekening beperkt uit veiligheidsoverwegingen
Loss	Het openbaar ministerie zal de politie opdracht geven om u te signaleren en in gijzeling te nemen voor 7 dagen, als u de betaling niet voldoet.
Loss	Om te voorkomen dat uw toegang tot de app wordt geweigerd
Loss	Ook zijn wij dan genoodzaakt het openbaar ministerie (OM) te verwittigen van uw nalatigheid.
Loss	zal er beslag gelegd worden op uw rekening.
Loss Deadline Time	Let wel op uw huidige betaalpas verloopt op 28-04-18
Loss Time	Binnenkort vervalt de toegang van een- of meerdere apparaten tot uw Mobiel Bankieren App.
Unpleasant_situation Time	Op dit moment maakt u nog geen gebruik van onze nieuwe omgeving
Loss Time	Uw ING Online zal binnenkort komen te verlopen
Unpleasant_situation Time	Het openstaande bedrag bij ons van u is tot op heden nog niet voldaan.
Unpleasant_situation Time	Uit ons klantenbestand is naar voren gekomen dat u, ondanks meerdere contactpogingen, nog gebruik maakt van een verouderde Rabopas.
Unpleasant_situation Time	Wij hebben u meerdere malen per brief verzocht om de betaling te voldoen.
Unpleasant_situation	Beslaglegging Bankrekening .
Unpleasant_situation	De vordering is overgedragen aan het Centraal Justitieel Incassobureau.
Unpleasant_situation	Hiermee willen wij u vermelden dat er mogelijk is geprobeerd een online betaling te verrichten met uw Card.
Unpleasant_situation	Mijn ICS en Card geblokkeerd
Unpleasant_situation	Uit onderzoek op uw Rabo Internetbankieren is gebleken dat u zich niet volgens de algemene voorwaarden heeft uitgelogd.
Unpleasant_situation	Uit ons klantenbestand is naar voren gekomen dat u, ondanks meerdere contactpogingen, nog gebruik maakt van een verouderde Rabopas. .
Time	Als klant wilt u duidelijk en tijdig genformeerd worden
Time	Het verifiren van uw rekening duurt ongeveer 5 minuten.

Continued on next page

Tabel 7 – continued from previous page

Urgency category	Text
Time	Op dit moment maken we al verschillende stappen om de nieuwe omgeving volledig naar het consument te brengen.
Time	U ontvangt de vernieuwde Rabopas binnen enkele werkdagen per post.