SVR - Webartikel 2012/5

Veiligheid van het internet

Welke problemen ondervinden de Vlamingen?

Marie-Anne Moreas

Vlaamse overheid
Studiedienst van de Vlaamse Regering
D/2011/3241/072

Samenvatting

Internetveiligheid is in het Vlaamse Gewest een probleem net zoals in andere Europese landen. Volgens de enquête 'Community Survey on ICT usage in Households and by Individuals' van 2010 werd een derde (33%) van de Vlaamse internetgebruikers het voorbije jaar geconfronteerd met één of meerdere veiligheidsproblemen zoals een computerinfectie, misbruik van persoonlijke informatie of schending van privacy, verschillende vormen van financiële schade of het in contact komen van kinderen met ongeschikte websites of potentieel gevaarlijke personen. Als we spam bij de internetproblemen rekenen, komen we tot vele hogere percentages. Twee derde (66%) van de internetgebruikers in het Vlaamse Gewest had vorig jaar immers last van ongewenste e-mails, dit is meer dan in andere Europese landen (EU27= 57%). Jongere internetgebruikers komen meer in contact met al deze internetproblemen dan oudere. In het Vlaamse Gewest ervaren meer internetgebruikers spam en minder internetgebruikers een computervirus dan in de EU27.

De meeste Vlaamse internetgebruikers zijn wat bezorgder over hun onlineveiligheid dan gemiddeld in de EU27 het geval is. Deze bezorgdheid van de Vlaming neemt duidelijk toe met de scholing.

Bijna twee derde (64%) van de Vlaamse internetgebruikers vermijdt bepaalde internettoepassingen om veiligheidsredenen. De Vlaamse internetgebruiker scoort binnen de EU hoog voor het vermijden van risicovolle onlinetoepassingen. Dit is volgens de Europese Commissie één van de obstakels om het sociale en economische potentieel van ICT te maximaliseren.

Een pluspunt is dat nu al een groot deel van de Vlaamse internetgebruikers minstens één "veiligheidstool" gebruikt om de privécomputer te beschermen (91%). Een antivirus en/of anti-spywareprogramma en een e-mailfilter om spam tegen te houden, zijn populairder bij de internetgebruikers van het Vlaamse Gewest dan bij deze in de EU27. Andere instrumenten, zoals firewalls of software voor ouderlijk toezicht of webfiltersoftware, worden in Vlaanderen minder gebruikt. Binnen de EU scoort het Vlaamse Gewest dan ook gemiddeld voor het gebruik van deze beveiligingstools door zijn burgers. Verder updaten slechts 87% van de Vlaamse bezitters minstens occasioneel hun beveiligingsproducten, tegen 92% van de EU27-bezitters. Hoe ouder en hoe lager geschoold, hoe kleiner de kans dat de beschikbare beveiligingsproducten geüpdatet worden in het Vlaamse Gewest. De oudere en in mindere mate de laag- en mediumgeschoolde Vlaamse internetgebruikers zijn er zich ook minder van bewust of zij al dan niet een veiligheidstool gebruiken.

Inleiding

In maart 2010 werd de 'Europa 2020'-strategie gelanceerd om uit de crisis te geraken en om de economie voor te bereiden op de uitdagingen van de volgende 10 jaar. Eén van de zeven deeldomeinen in het kader van het actieplan Europa 2020 is de 'Digitale agenda'. Het doel van deze agenda bestaat erin het sociale en economische potentieel van ICT – vooral internet – te maximaliseren, waardoor innovatie, economische groei en verbeteringen in het dagelijkse leven van burgers en bedrijven mogelijk worden.

De commissie heeft de belangrijkste obstakels voor de optimalisatie van het sociale en economische potentieel van ICT geïdentificeerd. Eén ervan is 'een groeiende cybercriminaliteit en het risico van weinig vertrouwen in netwerken'. Europeanen zullen zich maar ten volle engageren in steeds meer gesofisticeerde onlineactiviteiten als ze het gevoel hebben dat zijzelf en hun kinderen de netwerken volledig kunnen vertrouwen. Toepassingen zoals e-banking en e-health hebben geen succes zonder perfect betrouwbare systemen. Internet is een zeer kritische infrastructuur voor informatie geworden, zowel voor burgers als voor bedrijven. Het internet zelf is veilig en stabiel, maar de IT-netwerken en de terminals van eindgebruikers blijven kwetsbaar voor een heel scala aan evoluerende bedreigingen. Verder zijn er steeds meer databases en nieuwe technologieën die individuen op afstand controleren. Om de betrouwbaarheid van IT-netwerken en –systemen en het vertrouwen in deze te verhogen, worden op Europees niveau enkele acties aangekondigd. Van de lidstaten worden – idealiter - volgende acties verwacht.

- ➔ Er wordt een simulatie van een grootschalige aanval gepland waarbij de verhelpende strategieën worden getest.

- ➔ Tegen 2012 worden nationale alarmcentrales opgezet of aangepast aan het 'Europol cybercrime platform'. Verder moet een goed functionerend netwerk van Computer Emergency Response Teams (CERT's) op nationaal niveau worden uitgewerkt die heel Europa overspannen. De 'European Network and Information Security Agency' omschrijft de taak van deze CERT's als volgt: "Every single country that is connected to the internet must have capabilities at hand to effectively and efficient respond to information security incidents. But CERT's must do much more. They must act as primary security service providers for government and citizens. At the same time, they must act as awareness raisers and educators." CERT's moeten er dus voor zorgen dat op een effectieve en efficiënte wijze gereageerd wordt op incidenten waarbij de informatieveiligheid in het gedrang komt. Maar ze hebben via een bewust-makingsproces en via educatie ook een preventieve functie.

- ➔ Tegen 2013 zijn er hotlines voor het melden van beledigende of schadelijke online-inhoud, zijn er campagnes die mensen bewust maken van de onlineveiligheid voor kinderen, zijn er in scholen lessen over onlineveiligheid en worden providers van onlinediensten gestimuleerd om zelfregulerende maatregelen te treffen betreffende de onlineveiligheid voor kinderen.

In deze publicatie beschrijven we de veiligheidsproblemen die mensen ervaren bij internetgebruik. We onderzoeken hun bezorgdheid voor dergelijke problemen en gaan na welke acties zij ondernemen om deze problemen te vermijden. We plaatsen de cijfers voor het Vlaamse Gewest hierbij in een Europees perspectief. Meestal wordt het Vlaamse Gewest vergeleken met de EU27 en de buurlanden van België.[1]

[1] Statistieken voor de overige gewesten en de overige deelnemende EU-landen kunnen op eenvoudig verzoek bekomen worden bij de auteur.

1. Bronnen

'Veiligheid van het internet' is een ad-hocmodule in de Eurostat-vragenlijst 'Community Survey on ICT Usage in Households and by Individuals' van 2010. De data worden verzameld door de nationale instituten voor de statistiek of door ministeries. De deelnemende landen zijn de EU27-landen en ook IJsland, Noorwegen, Kroatië, Macedonië en Turkije.

In België organiseert de 'Algemene Directie Statistiek en Economische Informatie, FOD Economie, K.M.O., Middenstand en Energie' de enquête 'ICT- en internetgebruik bij huishoudens'. Er zijn twee methodes van gegevensverzameling: via een webapplicatie en via een papieren formulier. Deze schriftelijke bevraging of webenquête wordt afgenomen bij een deel van de respondenten van de Enquête naar de Arbeidskrachten (EAK). Na het afnemen van de EAK-enquête bepaalt de enquêteur op basis van de verjaardagen welk gezinslid de vragen over het ICT-gebruik dient te beantwoorden. De enquêteur overhandigt een papieren vragenlijst en een document met de nodige uitleg om via de webapplicatie deel te nemen. Na twee à drie weken wordt voor zover nodig een herinneringsbrief gestuurd.

De respons voor de ICT-enquête bedraagt in het Vlaamse Gewest 72,2% ten opzichte van de initiële brutosteekproef. In totaal namen 3.682 personen tussen 16 en 74 jaar uit het Vlaamse Gewest deel aan de enquête. Voor België namen 6.160 burgers deel en was de responsgraad 61,5%.

2. Resultaten

De vragen betreffende de veiligheid van het internet bij burgers hebben enkel betrekking op het gebruik van het internet in het voorbije jaar en voor privéredenen.

In een eerste deel beschrijven we de mate waarin de verschillende onlineveiligheids-problemen voorkomen. Vervolgens komt de bezorgdheid van de burger met betrekking tot het internetgebruik aan bod. We sluiten dit artikel af met de wijze waarop de burger een antwoord probeert te bieden op deze onlinebedreigingen.

We onderzoeken telkens de verschillen tussen bevolkingsgroepen in functie van de leeftijd en de opleiding.

2.1. Ondervonden problemen bij internetgebruik

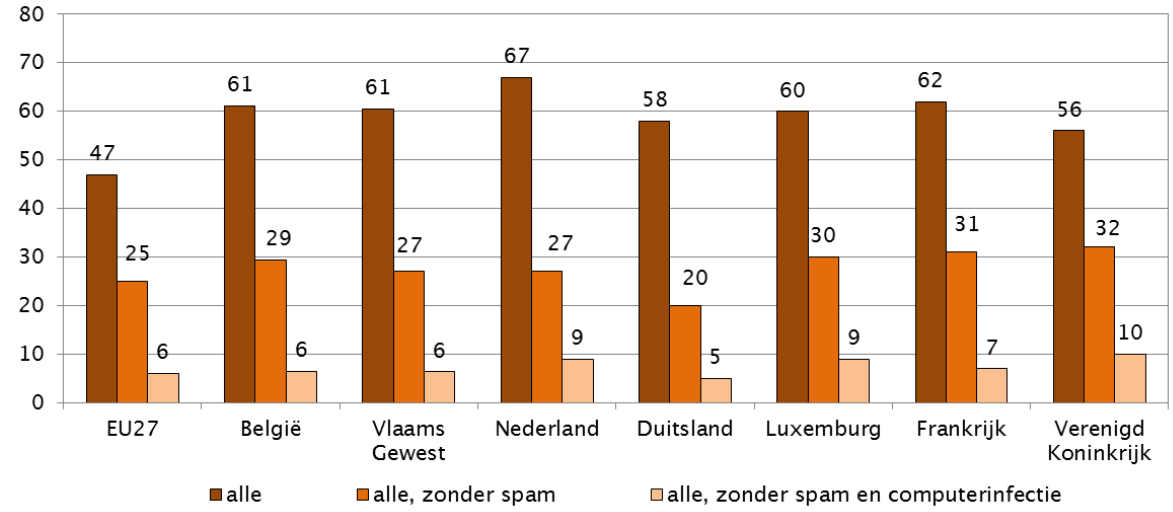
De respondent kan in de vragenlijst zes mogelijke problemen aanduiden die hij gedurende het voorbije jaar ervaren heeft. Deze zijn:

- spam: ongewenste e-mails of spam;
- computerinfectie: een besmetting met een virus of een andere computerinfectie, bijvoorbeeld een worm of een Trojaans paard, met een verlies van gegevens of tijd tot gevolg;
- onlinegevaren voor kinderen: de blootstelling van kinderen aan ongeschikte websites of het in contact komen van kinderen met potentieel gevaarlijke personen;
- schending van de privacy: misbruik van op het internet geplaatste persoonlijke informatie of andere vormen van schending van de privacy, waaronder misbruik van foto's, video's of van persoonlijke gegevens geplaatst op community websites;
- financiële schade door phishing of pharming: financiële schade als gevolg van de ontvangst van frauduleuze berichten ('phishing') of van het ongemerkt omleiden naar valse websites om gevoelige informatie te verwerven ('pharming');
- financiële schade door fraude: financiële schade als gevolg van frauduleuze betalingen via het internet.

Spam werd door 54% van de Vlamingen en door 40% van de EU27-burgers ervaren; een computerbesmetting door 23% van de Vlamingen en door 22% van de EU27-burgers. De overige categorieën van problemen worden door 1% tot 3% van de Vlamingen of EU27-burgers ervaren.

Volgens figuur 1 heeft 61% van de Vlamingen tussen 16 en 74 jaar in het voorbije jaar één of meerdere van de zes voormelde problemen ervaren. Hiermee neemt het Vlaamse Gewest een middenpositie in tegenover zijn buurlanden. In de EU27 werd maar 47% van de burgers geconfronteerd met één van deze zes problemen. Dit verschil is voornamelijk te verklaren door de sterkere aanwezigheid van spam in het Vlaamse Gewest en in zijn buurlanden dan in de EU27. Wanneer we spam buiten beschouwing laten, had in 2010 nog ruim een vierde van de Vlamingen minstens één van de vijf resterende problemen ervaren. In Luxemburg, Frankrijk en in het Verenigd Koninkrijk ligt dit percentage hoger, in Duitsland een stuk lager. In deze verschillen speelt het aandeel burgers dat een computervirus ervaarde, een rol. Zonder spam of een computerinfectie blijven nog vier indringende veiligheids-problemen over. 6% van de Vlamingen ervaarde minstens één van deze. In Nederland, Luxemburg en het Verenigd Koninkrijk is dat 9 tot 10%. In deze landen worden meer personen geconfronteerd met schending van de privacy en/of met financieel verlies. De cijfers over het voorkomen van deze problemen in de maatschappij geven ons een beeld van het maatschappelijke belang van deze problematiek. In wat volgt, onderzoeken we de kans dat een internetgebruiker geconfronteerd wordt met een veiligheidsprobleem.

Figuur 1 Aandeel burgers van 16 tot 74 jaar dat minstens één veiligheidsprobleem ervaren heeft in het voorbije jaar in functie van de opgenomen problemen (alle problemen, alle problemen min spam, alle problemen min spam en computervirus), 2010, EU27, Vlaams Gewest, België en buurlanden, in %



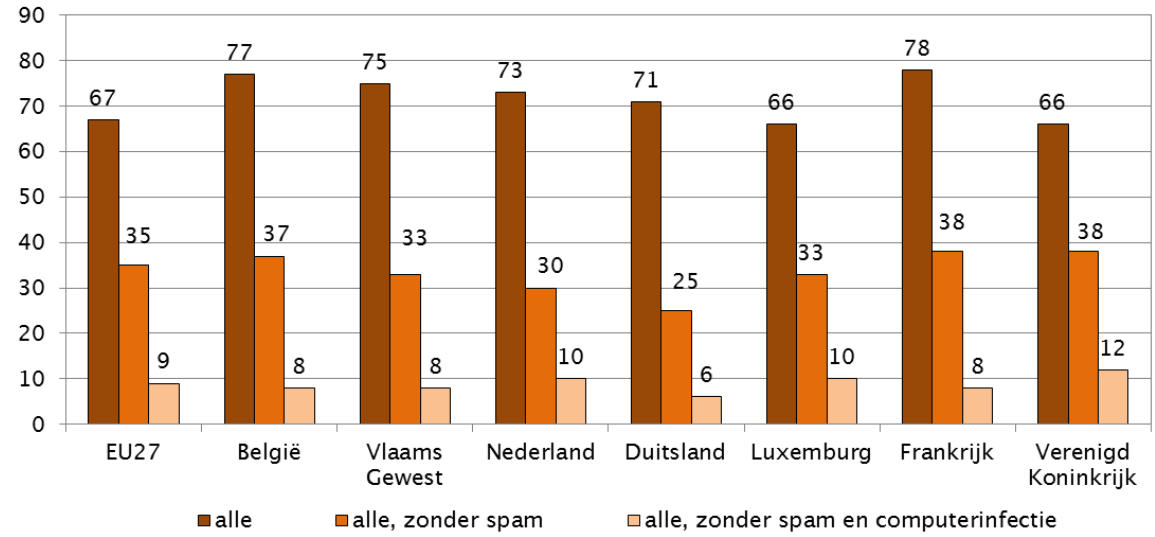
Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

Hoe groter het aandeel burgers dat gebruik maakt van het internet, hoe groter het aandeel burgers dat geconfronteerd kan worden met internetproblemen. Om de veiligheid van het internet in een land te beoordelen, herberekenen we de aandelen daarom alleen voor de internetgebruikers. Deze percentages liggen natuurlijk wat hoger. In 2010 had 28% van de online Vlamingen een computerinfectie ervaren (EU27= 31%) en 66% had spam gekregen (EU27= 57%). Misbruik van online geplaatste persoonlijke informatie of andere vormen van schending van de privacy kwamen voor bij 3% van de Vlaamse internetgebruikers (EU27= 4%) en 4% van de Vlaamse internetgebruikers zag dat kinderen blootgesteld waren aan ongeschikte websites of via het internet in contact kwamen met potentieel gevaarlijke personen (EU27= 3%). Financiële schade als gevolg van 'phishing' of 'pharming' kwam voor

bij 2% van de Vlaamse internetgebruikers (EU27= 2%) en 1% had financiële schade als gevolg van frauduleuze betalingen via het internet (EU27= 2%).

Volgens figuur 2 heeft in 2010 driekwart van de Vlaamse internetgebruikers tenminste één van de zes voormelde veiligheidsproblemen ervaren in het voorbije jaar, wat heel wat hoger is dan in de EU27. Het veelvuldig voorkomen van spam is de oorzaak van deze sterke aanwezigheid van internetproblemen in het Vlaamse Gewest: wanneer we spam buiten beschouwing laten, komen er namelijk minder internetproblemen voor in het Vlaamse Gewest (33% zonder spam) dan gemiddeld in de EU27 (35% zonder spam). Het percentage voor het voorkomen van tenminste één van de zes internetproblemen is bij de buurlanden alleen in Frankrijk nog hoger. In Luxemburg en in het Verenigd Koninkrijk wordt 'slechts' 66% van de internetgebruikers geconfronteerd met één van de zes veiligheidsproblemen die in de enquête werden aangeboden. Volgens figuur 2 zijn alleen de Duitse internetgebruikers beter af voor de drie groepen van internetproblemen (alle, alle zonder spam en alle zonder spam en computerinfectie).

Figuur 2 Aandeel internetgebruikers van 16 tot 74 jaar dat minstens één veiligheidsprobleem ervaren heeft in het voorbije jaar in functie van de opgenomen problemen (alle problemen, alle problemen min spam, alle problemen min spam en computervirus), 2010, EU27, Vlaams Gewest, België en buurlanden, in %



Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

Om deze resultaten beter te kunnen kaderen, onderzoeken we de samenhang tussen de internetpenetratie in een regio en het voorkomen van deze veiligheidsproblemen bij de 'internetgebruikers' van een regio. Het voorkomen van een veiligheidsprobleem wordt hierbij geoperationaliseerd als het aandeel internetgebruikers dat het probleem ervaren heeft in het voorbije jaar. In de analyses betrekken we de deelnemende landen aan de Eurostat-enquête en de 3 Belgische gewesten. We stellen vast dat spam meer voorkomt bij internetgebruikers uit landen met een hoge internetpenetratie. Dit geldt voor alle leeftijds- en opleidingsgroepen. Computerinfecties komen marginaal significant (p= 0,077, tweezijdige toets) vaker voor bij internetgebruikers uit landen met een lage internetpenetratie. De samenhang wordt sterker naarmate de internetgebruikers ouder of hoger geschoold zijn en is significant voor de 55- tot 74-jarigen en voor de hooggeschoolden. Voor het voorkomen van één van de vier andere problemen is er geen relatie met de internetpenetratie in de regio.

Tabel 1 Pearson product-momentcorrelaties tussen het aandeel internetgebruikers enerzijds en het aandeel internetgebruikers dat een veiligheidsprobleem ervaren heeft anderzijds, over de verschillende regio's, naar leeftijd en geslacht, 2010

			Leeftijd		
Probleem	Alle		16-24	25-54	55-74
Spam	**0,615**	***	**0,643** ***	**0,658** ***	**0,457** **
Virus	**-0,307**		-0,041	**-0,291**	**-0,376** *
Overige problemen	0,038		0,167	0,176	-0,078
			Opleiding		
Probleem	Alle		Laag	Medium	Hoog
Spam	**0,615**	***	**0,569** ***	**0,576** ***	**0,578** ***
Virus	**-0,307**		-0,176	**-0,326**	**-0,428** *
Overige problemen	0,038		0,074	0,073	-0,059

Noot: **In vet**: p<0,10; *** p<0,001; ** p<0,01, * p<0,05; tweezijdige toets; een kleinere p-waarde staat voor een meer betekenisvol verband. N= 33 of 34 behalve voor de correlatie tussen 'Overige problemen' voor de 55- tot 74-jarigen en internetgebruik waar N=28.

Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

In regio's waar meer internetgebruikers een computervirus hebben ervaren, hebben over het algemeen ook meer internetgebruikers één van de vier minder frequent voorkomende internetproblemen ervaren (r= 0,49, p= 0,003, N= 35)[2]. Het aandeel internetgebruikers dat geconfronteerd werd met een computervirus of met één van de vier minder frequent voorkomende internetproblemen, hangt niet betekenisvol samen met het aandeel internetgebruikers dat spam heeft ervaren in een regio.

Ten slotte onderzoeken we of de scholingsgraad en de leeftijd een impact hebben op de kans om een veiligheidsprobleem te ervaren. In het Vlaamse Gewest hangt spam het sterkst samen met de leeftijd en de opleiding. Door het bredere internetgebruik van jongeren en hooggeschoolden, en de gebrekkige mogelijkheden om spam te voorkomen, komen deze groepen van internetgebruikers waarschijnlijk meer in contact met ongewenste e-mails. Ook in de buurlanden en in de EU27 komen de online 55-plussers minder in contact met spam, al is deze relatie niet overal even sterk. Spam hangt ook in al de buurlanden en in de EU27 samen met de scholing. Een computerinfectie wordt in al de beschouwde regio's meer ervaren naarmate de leeftijd afneemt. De relatie met de opleiding is minder sterk tot onbestaande in de beschouwde regio's. De cijfers voor de overige problemen zijn minder eenduidig door de kleinere percentages. De 55- tot 74-jarigen komen in het Vlaamse Gewest wat minder in contact met deze problemen dan de andere leeftijdsgroepen; de verschillen voor opleiding zijn klein.

[2] De samenhangen betreffen samenhangen over regio's, die zeggen niets over de samenhangen op individueel niveau. Een voorbeeld. Over de regio's zou het kunnen dat het voorkomen van spam en van computervirussen niet samenhangt, omdat internetgebruikers in landen met veel spam ook meer risico lopen op computervirussen, maar zich er ook beter voor beschermen. Dit houdt niet in dat er op individueel niveau geen verband kan zijn tussen het voorkomen van spam en computervirussen. Dit zal onderzocht worden in een volgend artikel.

Tabel 2 Aandeel internetgebruikers dat een veiligheidsprobleem ervaart naar leeftijd en opleiding, 2010, EU27, Vlaams Gewest, België en buurlanden, in %

	Spam			Computerinfectie			Overige problemen		
	Leeftijd								
Land/regio	16-24	25-54	55-74	16-24	25-54	55-74	16-24	25-54	55-74
EU27	56	58	51	38	31	21	7	10	6
België	73	69	58	44	32	23	10	8	7
Vlaams Gewest	75	67	55	36	29	19	10	8	7
Nederland	77	71	55	34	24	14	11	12	6
Duitsland	67	71	57	29	22	15	6	6	-
Luxemburg	69	59	46	46	26	19	12	11	6
Frankrijk	69	72	64	44	35	24	-	10	-
Verenigd Koninkrijk	53	56	50	39	32	-	9	14	-
	Opleiding								
Land/regio	laag	medium	hoog	laag	medium	hoog	laag	medium	hoog
EU27	50	54	66	33	30	30	9	8	10
België	58	65	78	33	32	32	7	9	8
Vlaams Gewest	56	64	77	25	28	30	7	8	8
Nederland	61	67	75	25	23	22	9	9	12
Duitsland	61	66	77	27	20	20	8	5	7
Luxemburg	48	57	66	36	25	24	9	11	11
Frankrijk	60	76	82	34	37	31	8	7	9
Verenigd Koninkrijk	30	51	65	25	34	29	11	11	15

Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

2.2. Bezorgdheid om onlineveiligheid

Tabel 3 geeft weer hoe bezorgd de Vlaamse internetgebruiker is over zijn onlineveiligheid.

Voor elk van de zes vermelde problemen is 16 tot 26% van de Vlaamse internetgebruikers 'helemaal niet bezorgd'. Het aandeel niet-bezorgden is voor elk van deze problemen hoger in de EU27, Nederland en Luxemburg. De Franse internetgebruiker is minder bezorgd voor vijf van deze problemen (uitgezonderd spam). De Duitser en de Brit zijn minstens even bezorgd als de Vlaming. Uitzondering hierop is de onlineveiligheid van kinderen: in al onze buurlanden maakt de internetgebruiker zich minder zorgen om de inhoud of de personen waarmee kinderen online in contact komen.

Het aandeel niet-bezorgden daalt voor elk probleem in functie van de opleiding: online hooggeschoolden zijn vaker bezorgd dan online laaggeschoolden. Voor al de veiligheidsproblemen, uitgezonderd de veiligheid voor de kinderen, geldt dat ook in de EU27 en voor al de buurlanden. Voor leeftijd is deze trend minder duidelijk. De 25- tot 54-jarigen zijn minder vaak 'helemaal niet bezorgd' dan de jongeren. Ze zijn voor een mogelijk financieel verlies, voor de onlineveiligheid voor kinderen en voor de schending van de privacy ook bezorgder dan de ouderen. Dit geldt niet alleen voor het Vlaamse Gewest maar ook voor de meeste buurlanden.

Tabel 3 Aandeel internetgebruikers dat helemaal niet bezorgd is om een veiligheids-probleem voor de totale bevolking tussen 16 en 74 jaar en naar leeftijd en opleiding, 2010, EU27, Vlaams Gewest, België en buurlanden, in %

	Alle	Leeftijd			Opleiding			Alle	Leeftijd			Opleiding		
	burgers	16-24	25-54	55-74	laag	medium	hoog	burgers	16-24	25-54	55-74	laag	medium	hoog
	Virus of andere computerinfectie							**Spam**						
EU27	21	25	20	21	26	21	18	29	37	27	26	35	29	24
België	15	15	14	17	21	16	10	23	30	22	20	29	24	17
Vlaams Gewest	16	18	15	17	20	17	11	26	37	25	23	32	28	21
Nederland	45	53	43	44	50	46	39	50	66	48	46	54	53	44
Duitsland	10	17	9	9	16	9	8	16	29	15	11	23	15	14
Luxemburg	35	39	34	34	38	35	33	40	42	36	50	47	39	35
Frankrijk	23	26	20	26	26	23	16	22	28	18	27	30	20	10
Verenigd Koninkrijk	14	19	13	14	22	15	11	23	37	21	16	29	23	21
	Misbruik persoonlijke info en inbreuken op privacy							**Financieel verlies door phishing of pharming**						
EU27	28	32	26	30	39	25	23	36	45	34	35	48	33	32
België	19	18	18	23	24	20	14	20	24	19	22	26	20	16
Vlaams Gewest	21	21	20	25	26	22	17	23	31	20	26	29	24	19
Nederland	32	33	29	36	36	32	27	48	58	46	46	52	51	42
Duitsland	14	19	12	15	19	13	11	17	31	14	14	25	15	14
Luxemburg	37	34	35	43	41	36	34	51	52	50	55	55	50	49
Frankrijk	50	62	45	53	58	52	35	64	80	59	66	70	65	54
Verenigd Koninkrijk	12	16	11	12	24	12	10	16	21	15	13	22	15	15
	Financieel verlies door frauduleus gebruik van de kredietkaart							**Kinderen komen in contact met ongewenste websites of personen**						
EU27	35	46	32	33	48	33	28	42	51	38	48	48	40	41
België	21	28	19	23	28	22	15	20	22	18	28	26	21	15
Vlaams Gewest	24	32	21	28	31	24	19	19	22	16	26	25	21	13
Nederland	42	55	39	43	49	44	35	57	63	49	70	59	53	59
Duitsland	22	39	19	18	34	21	16	43	56	39	46	46	41	47
Luxemburg	46	50	43	51	53	45	41	50	41	50	55	47	48	54
Frankrijk	54	70	48	56	61	55	42	55	72	48	60	59	57	47
Verenigd Koninkrijk	12	18	10	-	22	12	8	25	27	23	28	23	22	30

Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

Vervolgens exploreren we de samenhang tussen de mate van internetpenetratie in een regio en het aandeel van de onlineburgers dat enige bezorgdheid aangeeft. Hier zijn verbanden in twee richtingen mogelijk. Een grotere internetpenetratie kan zorgen voor een grotere bewustwording voor dergelijke problemen, maar ook voor een grotere bewustwording van manieren waarop de internetgebruiker zich hiervoor kan beschermen. We hebben bijgevolg geen duidelijke verwachting over het mogelijke verband tussen het aandeel onlineburgers in een regio en de bezorgdheid van deze onlineburgers. Volgens de Pearson product-momentcorrelaties zijn deze samenhangen er ook niet ($p< 0,05$).

Hieruit volgt de vraag of er over de regio's heen een verband is tussen het aandeel internetgebruikers dat een internetprobleem heeft ervaren en de bezorgdheid voor deze problemen. Het antwoord is[3]: hoe groter het aandeel internetgebruikers dat met spam geconfronteerd wordt, hoe groter de bezorgdheid voor alle internetproblemen uitgezonderd een computervirus. Het voorkomen van een computervirus of een van de vier overige internetproblemen, hangt niet betekenisvol samen met de bezorgdheid. Het is interessant om te zien dat de bezorgdheid voor de meeste problemen samenhangt met spam; een internetprobleem dat minder effectief aangepakt kan worden dan een computervirus. Hangt de bezorgdheid dan samen met de effectieve dreiging wanneer de internetgebruiker zich niet zou beschermen voor de internetproblemen?

[3] De Pearson product-momentcorrelatie tussen het aandeel internetgebruikers die spam ervaren hebben en het aandeel internetgebruikers dat niet-bezorgd is voor elk van de internetproblemen, is voor spam: r= -0,38, p= 0,03; voor misbruik van persoonlijke info en inbreuken op de privacy: r= -0,39, p= 0,02; voor financieel verlies door phishing of pharming: r= -0,30, p= 0,08; voor financieel verlies door frauduleus gebruik van de kredietkaart: r= -0,48, p= 0,00 en voor onlinegevaren voor kinderen: r= -0,35, p= 0,04.

Via een principale componentenanalyse voor het aandeel 'niet-bezorgden' voor de verschillende internetproblemen, vinden we één component die 75% van de totale variantie verklaart. Het aandeel bezorgden voor al deze internetproblemen, uitgezonderd computervirus (lading= 0,56), worden goed vertegenwoordigd door deze component (lading≥ 0,86), 'bezorgdheid in de regio voor internetproblemen' genoemd. Deze bezorgdheid in de regio is hoger naarmate meer personen spam ervaren in deze regio (N= 35, r= -0,41, p= 0,014), en hangt niet samen met het aandeel personen dat problemen ondervindt met een virus of met de overige internetproblemen. Het Vlaamse Gewest, Duitsland en het Verenigd Koninkrijk hebben eerder bezorgde burgers. Luxemburg, Nederland en Frankrijk minder bezorgde burgers.

2.3. Verdedigingsmechanismen tegen onlinebedreigingen

Mensen kunnen op verschillende manieren omgaan met onlinerisico's. Ze kunnen bepaalde situaties vermijden die volgens hen een verhoogd risico inhouden. Hierdoor wordt niet alleen het risico vermeden, maar missen ze ook de voordelen van deze internet-toepassingen. De Digitale Agenda van Europa vindt dit niet de ideale reactie op lange termijn. De Europese Commissie wil de onlineveiligheid verhogen zodat Europeanen zich ten volle kunnen engageren in steeds meer gesofisticeerde onlineactiviteiten. De burgers kunnen ook enkele acties ondernemen om de eigen veiligheid te verhogen zonder dat ze de eigen onlineactiviteiten al te sterk moeten inperken. Zo kunnen ze software of hardware gebruiken om de eigen computer en de eigen gegevens te beveiligen. Wat doen de Vlamingen en Europeanen om onlinerisico's te vermijden?

2.3.1. Vermijden van onlinetoepassingen met een verhoogd risico

Volgende onlinetoepassingen werden in de enquête opgenomen:

- bestellen of kopen van goederen of diensten voor privégebruik;
- bankieren via internet zoals het online beheren van bankrekeningen;
- persoonlijke informatie beschikbaar stellen via onlinegemeenschappen voor het uitbouwen van sociale en professionele netwerken, bijvoorbeeld via Facebook of Twitter;
- online communiceren met openbare diensten en administraties;
- downloaden van software, muziek, videobestanden, spelletjes of andere data-bestanden;
- het gebruiken van internet met mobiele apparatuur, bijvoorbeeld een laptop, via een draadloze verbinding op andere plaatsen dan thuis.

Tabel 4 Aandeel internetgebruikers dat om veiligheidsredenen één van de risicovolle onlineactiviteiten in zijn privégebruik heeft vermeden in het voorbije jaar, 2010, EU27, Vlaams Gewest, België en buurlanden, in %

		Leeftijd			Opleiding		
Regio	Allen	16-24	25-54	55-74	laag	medium	hoog
EU27	49	44	51	51	50	47	52
België	58	53	58	63	55	57	61
Vlaams Gewest	64	55	64	68	61	62	68
Nederland	49	43	51	48	45	47	56
Duitsland	54	46	56	56	49	55	59
Luxemburg	49	49	49	49	49	48	50
Frankrijk	60	55	62	58	58	64	60
Verenigd Koninkrijk	41	39	40	46	38	41	42

Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

In het Vlaamse Gewest heeft ongeveer twee derde (64%) van de internetgebruikers één van deze risicovolle activiteiten om veiligheidsredenen niet uitgevoerd gedurende het voorbije jaar. Dit aandeel ligt een stuk hoger dan in de EU27 (49%) of in de meeste buurlanden. De oudere en de hooggeschoolde internetgebruikers hebben in het Vlaamse Gewest vaker één of meerdere onlineactiviteiten vermeden om veiligheidsredenen. Deze samenhang met leeftijd en opleiding vinden we niet in alle regio's terug.

De verschillen over de onlineactiviteiten zijn echter groot. De activiteiten die door het grootste aandeel Vlaamse internetgebruikers vermeden worden, zijn: het beschikbaar stellen van persoonlijke informatie via onlinegemeenschappen (39%), het bestellen en kopen van goederen en diensten via het internet (30%) en het downloaden van software, muziek, videobestanden, spelletjes of andere databestanden (25%). De online Vlamingen vermijden deze activiteiten vaker dan de internetgebruikers in de EU27 of uit de buurlanden. De overige onlineactiviteiten worden door 10 tot 16% van de Vlaamse internetgebruikers vermeden. De online Vlaming vermijdt minder e-banking en meer het internetgebruik via mobiele apparatuur dan de gemiddelde EU-internetgebruiker. Voor het vermijden van communicatie met de overheid is de situatie in het Vlaamse Gewest vergelijkbaar met de EU27.

Over het algemeen vermijden vooral de oudere internetgebruikers in het Vlaamse Gewest en in de EU27 de risicovolle internettoepassingen. Dit geldt niet voor e-banking en voor de communicatie met openbare diensten en de overheid. Jongeren en ouderen vermijden in het Vlaamse Gewest deze internettoepassingen vaker dan de middengroep van 25 tot 54 jaar. Jongeren van 16 tot 24 jaar hebben waarschijnlijk ook minder direct nut van e-banking en e-government dan de ouderen. De Vlaamse hooggeschoolden vermijden eerder het ter beschikking stellen van persoonlijke informatie via onlinegemeenschappen en het downloaden van software, muziek, videobestanden, spelletjes of andere databestanden. Laaggeschoolden vermijden eerder het aankopen/verkopen van goederen en diensten, e-banking en e-government. Deze relatie met de socio-demografische kenmerken is niet steeds in alle regio's in dezelfde richting.

Volgens een principale componentenanalyse laden de regionale aandelen van internetgebruikers die deze activiteiten vermeden op één factor die 72% van de totale variantie verklaart en waar al de variabelen hoog op laden (lading online bankieren = 0,68, voor de overige activiteiten is de lading minstens gelijk aan 0,83). Deze component geeft aan hoeveel internetgebruikers de verschillende onlineactiviteiten vermijden in de regio's. Het vermijden van onlineactiviteiten hangt over de regio's niet samen met de mate van bezorgdheid in de regio, maar wel met het aandeel internetgebruikers dat geconfronteerd werd met spam ($r= 0,48$, $p= 0,004$, $N= 35$) en met de vier overige en indringende problemen ($r= 0,51$, $p= 0,002$, $N= 35$). In het volgende deel onderzoeken we waar het Vlaamse Gewest zich situeert voor de twee soorten van coping, namelijk het vermijden van onlineactiviteiten versus het gebruiken van veiligheidstools.

2.3.2. Beveiligen van de eigen computer

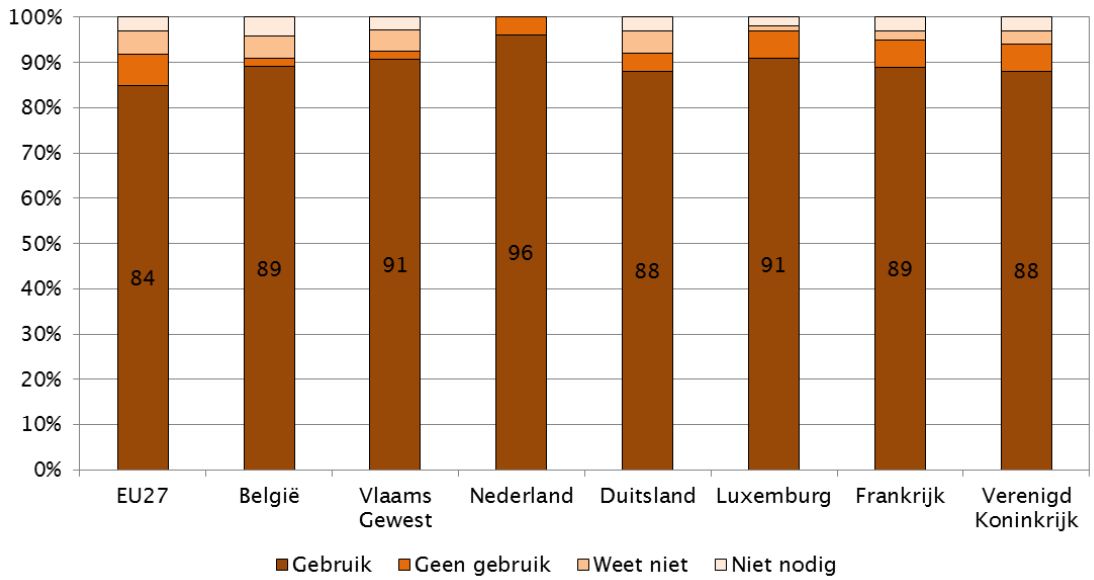
Om onlinerisico's te minimaliseren zonder in te boeten op de voordelen van de onlineactiviteiten, kan de internetgebruiker verschillende veiligheidstools inzetten. De bevraagde veiligheidstools zijn:

- een antivirus en/of anti-spyware programma;
- een hardware firewall, zoals een DSL- of kabelrouter of een software firewall, zoals ZoneAlarm;
- een e-mailfilter om spam tegen te houden;
- software voor ouderlijk toezicht of webfiltersoftware;
- andere software of hardware.

9 op de 10 online Vlamingen gebruikten in 2010 één van deze veiligheidstools om de privécomputer te beschermen. Dit is hoger dan in de EU27 en iets beter dan de percentages in de meeste buurlanden. Luxemburg doet het even goed als het Vlaamse

Gewest, Nederland doet het beter. De Nederlander is zich er ook meer van bewust of hij al dan niet gebruik maakt van deze tools.

Figuur 3 Aandeel internetgebruikers dat minstens één veiligheidstool gebruikt om de privécomputer te beschermen, 2010, EU27, Vlaams Gewest, België en buurlanden, in %



Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

Tabel 5 Aandeel internetgebruikers dat een veiligheidstool gebruikt om de privécomputer te beschermen, 2010, EU27, Vlaams Gewest, België en buurlanden, in %

	Virus*	Firewall	Spamfilter	Filtersoftware	Ander	Weet niet
EU27	71	48	34	9	2	11
België	82	38	35	7	5	5
Vlaams Gewest	83	34	40	4	5	7
Nederland	79	64	59	11	1	12
Duitsland	62	64	40	6	-	9
Luxemburg	77	60	52	16	3	12
Frankrijk	77	57	39	15	4	12
Verenigd Koninkrijk	75	55	40	14	2	10

Noot:
*: een antivirus en/of anti-spyware programma.

Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

Het aandeel personen dat bewust deze tools niet gebruikt, verschilt weinig wat leeftijd of opleiding betreft. De jongere of hogergeschoolde online Vlaming weet vaker of hij een veiligheidstool gebruikt dan de oudere of lagergeschoolde Vlaming. In die zin zouden educatie en bewustmakingsacties naar bepaalde bevolkingsgroepen nuttig kunnen zijn.

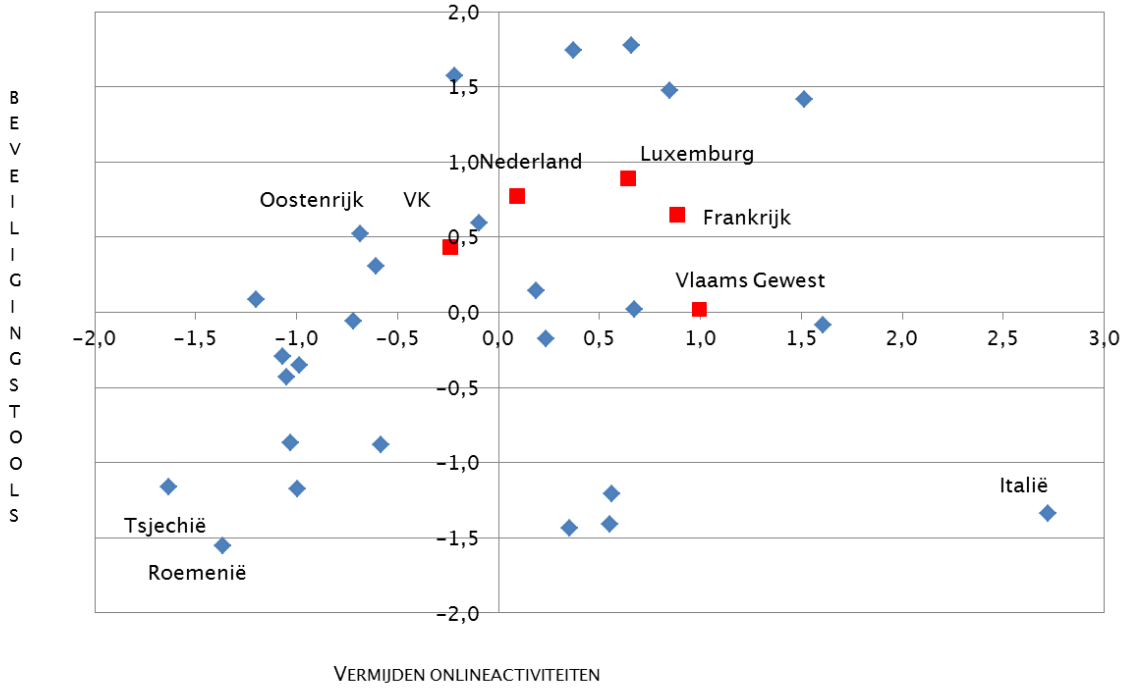
Een groter aandeel van de internetgebruikers van het Vlaamse Gewest dan van de EU27 maakt gebruik van een antivirus en/of anti-spywareprogramma en van een e-mailfilter om spam tegen te houden. Voor het antivirus en/of anti-spywareprogramma scoort het Vlaamse Gewest ook hoog in vergelijking met zijn buurlanden, wat niet het geval is voor de e-mailfilter om spam tegen te houden. Voor een hardware firewall, zoals een DSL- of

kabelrouter of een software firewall, zoals ZoneAlarm, scoort het Vlaamse Gewest lager dan de EU27 of zijn buurlanden. Software voor ouderlijk toezicht of een webfiltersoftware wordt in het Vlaamse Gewest heel wat minder gebruikt dan in de EU27 of in de buurlanden.

Via een principale componentenanalyse vinden we opnieuw één variabele die een goede weergave is voor de aandelen van internetgebruikers die zich in de regio's beschermen met elk van deze beveiligingsinstrumenten. Deze component verklaart 69% van de totale variantie, en representeert al de bekende instrumenten goed (ladingen ≥0,80). De ongedefinieerde categorie 'andere' laadt laag (lading= 0,53). Deze component, 'penetratie van beveiligingstools in een regio' genoemd, hangt zeer sterk samen met de internetpenetratie in de regio (r= 0,79, p<0,001, N= 30) en met het aandeel internetgebruikers dat geconfronteerd werd met spam (r= 0,41, p= 0,02, N= 31). De bezorgdheid over internetproblemen hangt niet samen met het gebruik van deze beveiligingsinstrumenten. Verder is de relatie tussen het vermijden van onlineactiviteiten en het gebruiken van beveiligingsinstrumenten in de regio niet betekenisvol (r= 0,24, p= 0,19, N= 31).

Ten slotte gaan we na waar het Vlaamse Gewest en zijn buurlanden zich situeren voor beide vormen van coping. Uit figuur 4 blijkt dat het Vlaamse Gewest en de meeste van zijn buurlanden zich bevinden in het tweede kwadrant waar beide vormen van coping meer dan gemiddeld ingeburgerd zijn. Het Vlaamse Gewest situeert zich voor de beveiligingstools rond het gemiddelde. In het Verenigd Koninkrijk gaan minder mensen de onlineactiviteiten vermijden. Voor Duitsland hebben we alleen een cijfer voor het vermijden, wat overeenkomt met het cijfer in het Vlaamse Gewest.

Figuur 4 Spreidingsdiagram voor de scores op de componenten 'vermijden van risicovolle onlineactiviteiten' en 'gebruiken van beveiligingsinstrumenten', 2010, internationale vergelijking



Noot: Rood vierkant: het Vlaamse Gewest of één van zijn buurlanden; blauwe ruit: andere EU-landen; 0 is het gemiddelde voor de component; negatieve cijfers houden in dat in deze regio minder gebruik wordt gemaakt van deze coping strategie, positieve meer.

Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

Een beveiligingsinstrument bezitten is echter niet voldoende. Het is minstens even belangrijk dat dit instrument regelmatig een update krijgt. De Vlaamse internetgebruikers zijn vrij laks in het updaten van hun beveiligingsproducten: slechts 87% van de Vlamingen tegen 92% van de EU27-burgers updaten één of meerdere van deze tools minstens occasioneel. In de buurlanden, uitgezonderd Frankrijk, updaten meer internetgebruikers hun beveiligingsinstrumenten. Hoe ouder en hoe minder geschoold, hoe kleiner de kans dat de beschikbare tools geüpdatet worden in het Vlaamse Gewest. Voor opleiding is deze trend vrijwel in alle beschouwde regio's aanwezig. Dit geldt niet voor leeftijd.

Tabel 6 Aandeel internetgebruikers dat minstens occasioneel updates voor zijn beveiligingsproducten installeert, 2010, EU27, Vlaams Gewest, België en buurlanden, in %

		Leeftijd			Opleiding		
	Alle	16-24	25-54	55-74	laag	medium	hoog
EU27	92	92	92	90	88	92	94
België	88	91	88	85	84	89	90
Vlaams Gewest	87	91	87	80	82	87	90
Nederland	93	93	94	90	88	93	96
Duitsland	93	93	94	92	91	93	95
Luxemburg	94	97	94	90	93	94	94
Frankrijk	85	84	86	83	82	87	88
Verenigd Koninkrijk	93	91	93	92	89	92	95

Bron: 'Community Survey on ICT Usage in Households and by Individuals', 2010, Eurostat, Belgische data: ADSEI, bewerking SVR

Uitleiding

Volgens de enquête 'Community Survey on ICT usage in Households and by Individuals' komt spam duidelijk veel voor bij Vlaamse internetgebruikers (66%). Verder werd in 2010 een derde (33%) van de online Vlamingen geconfronteerd met minstens één van volgende problemen: computerinfectie, misbruik van persoonlijke informatie of schending van de privacy, verschillende vormen van financiële schade of het in contact komen van kinderen met ongeschikte websites of potentieel gevaarlijke personen. Bij de online Vlamingen komen jongeren en hooggeschoolden meer in contact met deze veiligheidsproblemen dan ouderen of laaggeschoolden. Europa vraagt aandacht voor deze problematiek om het sociale en economische potentieel van ICT te maximaliseren.

Meer dan 9 op de 10 online Vlamingen gebruiken een veiligheidstool. Dit aandeel is hoger dan in de EU27. De online Vlaming gebruikt in vergelijking met de EU27-burger vaker een antivirus en/of anti-spywareprogramma en een e-mailfilter om spam tegen te houden. Voor een firewall of het gebruik van software voor ouderlijk toezicht of webfiltersoftware scoort het Vlaamse Gewest lager dan de EU27 en dan de buurlanden. Voor de software voor ouderlijk toezicht is dat des te opvallender omdat 81% van de online Vlamingen zich zorgen maakt over de inhoud en de personen waarmee kinderen online in contact komen. Wellicht kunnen de geplande maatregelen betreffende de onlineveiligheid voor kinderen, waaronder bewustmakingscampagnes en lessen over onlineveiligheid in het onderwijs, hier een bijdrage leveren.

De Vlaamse oudere en lagergeschoolde internetgebruikers weten in vergelijking met de andere internetgebruikers vaker niet of ze een veiligheidstool gebruiken. Van de mensen die een veiligheidstool gebruiken, zijn de Vlamingen lakser in het updaten van deze tools dan de EU27-burgers. Hoe ouder en hoe lagergeschoold, hoe kleiner de kans dat de beschikbare tools geüpdatet worden in het Vlaamse Gewest. Hier is een emancipatorische rol weggelegd voor de Computer Emergency Response Teams die de Europese Commissie

tegen 2012 wil oprichten. Zij moeten een bewustmakingsproces op gang brengen en gepaste opleidingen organiseren.

Ten slotte onderzochten we de onderlinge samenhang tussen de ervaren problemen, de bezorgdheid en het gekozen coping mechanisme. Hoe groter de internetpenetratie in een regio, hoe meer internetgebruikers er beveiligingstools gaan gebruiken. Zijn de burgers uit regio's met een hogere internetpenetratie beter op de hoogte van de internetproblemen en van de tools om deze te voorkomen en gaan ze zich daarom beter beschermen? En zou het risico op internetproblemen hoger zijn in regio's met een hogere internetpenetratie als ze zich niet beter zouden beschermen? De mogelijke relaties tussen de internetpenetratie in een regio en de aanwezigheid van internetproblemen, leidt tot de hypothese dat de internetpenetratie sterker zal samenhangen met problemen die niet door beveiligingstools kunnen voorkomen worden. De resultaten geven inderdaad aan dat een grotere internetpenetratie samenhangt met een sterkere aanwezigheid van spam en niet met de aanwezigheid van de overige internetproblemen. Spam is volgens dit exploratief onderzoek ook sterk gerelateerd aan de overige variabelen: hoe groter het aandeel personen dat spam ervaren heeft, hoe groter het aandeel internetgebruikers dat bezorgd is voor internetproblemen of dat elk van de coping strategieën heeft gebruikt. We veronderstelden hierbij dat spam minder beïnvloedbaar is door de coping strategieën en in die zin een weerspiegeling zou kunnen zijn van het reële risico op internetproblemen in de regio, wanneer de burgers zich niet zouden beschermen. De bezorgdheid en het aandeel gebruikers van coping strategieën zou in die zin samenhangen met het reële risico op internetproblemen. Deze hypothesen verdienen verdere toetsing.

Dit artikel geeft ons nog geen inzicht in samenhangen op individueel niveau. De samenhang tussen de ervaren problemen, de bezorgdheid of het gekozen coping mechanisme enerzijds en de breedte van het internetgebruik, de ICT-vaardigheid en andere verklarende factoren op individueel niveau anderzijds, zouden ons meer inzicht kunnen bezorgen in de processen die een rol spelen bij onlineveiligheid. Dit zal later worden onderzocht voor het Vlaamse Gewest.

Literatuurlijst

European Network and Information Security Agency, http://www.enisa.europa.eu/, geraadpleegd 11/01/2012.

Europese Commissie, *Europa 2020*, http://ec.europa.eu/europe2020/index_nl.htm, geraadpleegd 11/01/2012.

Europese Commissie, Digital *Agenda for Europe*, http://ec.europa.eu/information_society/digital-agenda/index_en.htm, geraadpleegd 11/01/2012.

Eurostat, *Europese cijfers*, http://epp.eurostat.ec.europa.eu/, geraadpleegd eind 2011.

Eurostat (2010). *Community survey on ICT usage in households and by individuals 2010, Eurostat Model Questionnaire* (version 3.2). http://epp.eurostat.ec.europa.eu/, geraadpleegd 11/01/2012.