MEASURING COST AND IMPACT OF CYBERCRIME IN BELGIUM (BCC): D.3.1.1.RISK PERCEPTION MONITOR REPORT (1ST WAVE, 2015)

Authors: Prof. dr. Pieter Verdegem (Pieter.Verdegem@UGent.be), Evert Teerlinck & Ewoud Vermote

Research Group: iMinds-MICT, Ghent University

Date: October 5, 2015

Het onderzoek dat tot deze resultaten leidde, werd gesubsidieerd door het Federaal wetenschapsbeleid via het contract nr BR/132/A4/BCC

PREFACE

While offering immense opportunities to the Belgian economy and society, the digital transition has also revealed various old and new threats in the form of cybercrime. It can compromise public and national security transportation, communication, e-commerce, and financial, emergency and other services that rely on digital information and infrastructure. Governments need to make informed decisions capable of protecting internet users against cyber threats and thus promoting economic growth. To this day, however, very little research has been done concerning the impact on the Belgian internet population, caused by cybercrime. This lack of information could lead to uninformed policies and inconsistent assessment of the issues at hand.

Given the far-reaching impact of cybercrime, efficient and effective mitigation measures involve various government sectors in addition to international cooperation. Foreseeing the need for scientific studies in this field, the Federal governmental agreement of 2011 affirmed that relevant stakeholders in combating cybercrime should be consulted. A National Cyber Security Strategy was adopted end 2012, stipulating that any action in this area shall be based on informed decision-making. End 2013 it was decided to create a Belgian Cyber Security Centre (CCSB). Fighting cybercrime is a major challenge and requires policy makers to be well acquainted with imminent threats. Therefore, investigating the magnitude and impact of this forms the primary goal of current study. A multidisciplinary research on the cost and impact of cybercrime will support the elaboration and implementation of efficient federal public policies allowing Belgium to take a strategic place on the international scene.

In 2014, a four-year interdisciplinary Belspo (Belgian Science Policy) Brain-be research project was set up with the cooperation of the B-CCENTRE (KU Leuven), ICRI (KU Leuven), Distrinet (KU Leuven), COSIC (KU Leuven) and MICT (UGent) on the cost and impact of cybercrime on the general population, the industry and the government in Belgium ('BCC project: Measuring Cost and Impact of Cybercrime in Belgium'). The project aims to demystify cybercrime and reach an objective, realistic and up-to-date picture of cybercrime related phenomena and their ramifications in Belgium and their evolution over time. The research will deliver a better informed and scientifically based view on the threats, and will provide strategic insights and guidelines to policy makers on how to advance the implementation of principles integrated in the Belgian National Cyber Security Strategy. The project involves both engineers to scrutinize the effectiveness of countermeasures, economists to calculate the (financial) impact of cybercrime, and social scientists to assess the subjective risk perception processes.

The work is performed in coordination by different research departments of different Belgian universities in parallel work packages, under the guidance of the Follow-up Committee of Belspo. Current research report forms the end-product of work package number three within the BCC project, which was executed by the Research Group for Media and ICT (iMinds-MICT), a research center affiliated to the Department of Communication Studies at Ghent University. Work package (WP3) three examines the cost and impact of cybercrime on the general Belgian population by means of quantitative research. It aims for the development and validation of a risk perception monitoring tool for mapping public risk perception levels concerning cybercrime and various related concepts (internet use, confidence in internet safety, severity and probability of threats, preventive behavior). Furthermore, core target groups are identified and defined for risk communication efforts by means of the quantitative data. The results of the survey are summarized in an accessible way, and thus provide useful information for diverse stakeholders.

We owe gratitude to Belspo for funding this research and to our partners within the BCC project for their support. Last but not least, we also want to thank all of the respondents for having filled out the survey. Without these respondents, who openly shared with us their online experiences, this report would not have been possible.

TABLE OF CONTENTS

PREFACE 2

TABLE OF CONTENTS 4

FIGURES AND TABLES 6

EXECUTIVE SUMMARY 9

Introduction 11

Theoretical perspectives 13

1. Cybercrime: definition and scope 13

2. Protection Motivation Theory 14

3. Internet security profiling 15

Methodology 16

1. Sample 16

2. Measures 20

2.1. Online activity 20

2.2. Being informed 20

2.3. Confidence in the safety of the internet 20

2.4. Safety of internet-related activities 21

2.5. Severity and probability of cybercrime forms 21

2.6. Cybercrime victimization 21

2.7. Safety measures 21

2.8. Theoretical model 22

2.9. Socio-demographic variables 23

3. Procedure 23

Survey results 25

1. Profiling the Belgian internet user 25

1.1. Online activity 25

1.2. Security behavior 30

1.3. Conclusion 36

1.4. Profiles of the internet users 37

A. Profile 1 - The conscious internet users 37

B. Profile 2 - The overly confident internet users 39

C. Profile 3 - The inexperienced internet users 41

D. Profile 4 - The resolved internet users 43

1.5. Conclusion 44

2. Cybercrime victimization 45

2.1. Viruses 46

2.2. Scams 52

2.3. Hacking 56

2.4. Governmental surveillance and corporate surveillance 59

2.5. Unwanted content and/or behavior 65

2.6. Financial impact 69

2.7. Conclusion 71

3. Risk perception monitoring tool 72

3.1. PMT in an internet security context 72

3.2. Perceived information and intention to perform security related behavior 73

3.3. PMT and the four user profiles 74

3.4. Conclusion 78

4. Recommendations for risk communication 79

4.1. Target groups 79

4.2. Topics and content 79

4.3. Conclusion 80

Discussion 81

Conclusion 82

Future research 84

REFERENCES 85

APPENDIX – SURVEY AS LAUNCHED 88

FIGURES AND TABLES

Figure 1: *Theoretical model* 15

Figure 2: *Distribution by gender* 16

Figure 3: *Distribution by age* 17

Figure 4: *Distribution by education level* 17

Figure 5: *Distribution by employment situation* 18

Figure 6: *Distribution by family situation* 18

Figure 7: *Distribution by residence* 19

Figure 8: *Online activity: frequency of internet use* 25

Figure 9: *Online activity: activities undertaken* 27

Figure 10: *Online activity: safety of activities* 29

Figure 11: *Security measures* 30

Figure 12: *Number of security measures one takes* 33

Figure 13: *Number of threats for which one seeks protection* 33

Figure 14: *Cybercrime victimization* 45

Figure 15: *Cybercrime victimization (combined)* 46

Figure 16: *Occurrence of viruses (count)* 47

Figure 17: *Damages of viruses* 48

Figure 18: *Way of obtaining viruses* 49

Figure 19: *Other effect of the virus* 49

Figure 20: *Kind of virus* 50

Figure 21: *Reporting of viruses* 51

Figure 22: *Occurrence of scams (count)* 53

Figure 23: *Occurrence of scams (when)* 53

Figure 24: *Kind of scam* 54

Figure 25: *Reporting of scams* 55

Figure 26: *Occurrence of hackings (count)* 57

Figure 27: *Subject of hacking* 58

Figure 28: *Reporting of hacking* 58

Figure 29: *Occurrence of governmental surveillance (count)* 61

Figure 30: *Occurrence of corporate surveillance (count)* 62

Figure 31: *Governmental surveillance: act of intrusion* 62

Figure 32: *Corporate surveillance: act of intrusion* 63

Figure 33: *Reporting of governmental surveillance* 64

Figure 34: *Reporting of corporate surveillance* 64

Figure 35: *Occurrence of unwanted content and behavior (count)* 66

Figure 36: *Kind of unwanted content and behavior* 67

Figure 37: *Reporting of unwanted content and behavior* 68

Figure 38: *Cost of cybercrime* 69

___

Table 1: *Rotated factor loadings of online activity sum variables* 28

Table 2: *Frequency table of security measures taken against internet threats* 31

Table 3: *Rotated factor loadings of security behavior sum variables* 34

Table 4: *Rotated factor loadings of threat security behavior sum variables* 35

Table 5: *Breakdown by residence for virus victimization* 46

Table 6: *Breakdown by residence for scam victimization* 52

Table 7: *Breakdown by residence for hacking victimization* 56

Table 8: *Breakdown by age category for governmental surveillance victimization* 60

Table 9: *Breakdown by age category for corporate surveillance victimization* 61

Table 10: *Breakdown by residence for unwanted content and/or behavior victimization* 65

Table 11: *Breakdown by age category for unwanted content and/or behavior victimization* 66

Table 12: Regression model where intention to adopt internet security measures is predicted by means of PMT variables, socio-demographic variables and user profile 73

Table 13: Regression model where intention to adopt internet security measures is predicted by means of PMT variables and socio-demographic variables for Profile 1 - The conscious internet users 75

Table 14: Regression model where intention to adopt internet security measures is predicted by means of PMT variables and socio-demographic variables for Profile 2 - The overly confident internet users 75

Table 15: Regression model where intention to adopt internet security measures is predicted by means of PMT variables and socio-demographic variables for Profile 3 - The inexperienced internet users 76

Table 16: Regression model where intention to adopt internet security measures is predicted by means of PMT variables and socio-demographic variables for Profile 4 – The resolved internet users 77

EXECUTIVE SUMMARY

Within this research report we make use of a typology of cybercrime types, based on a literature review, other monitoring instruments and expert consultations. This categorization distinguishes between: (1) viruses; (2) scams; (3) hacking; (4) governmental surveillance; (5) corporate surveillance; and (6) unwanted content and/or behavior.

On the theoretical level, this research has used the Protection Motivation Theory (PMT, Rogers, 1975) as a guiding framework. The PMT helps in understanding the process individuals go through in deciding which security behaviors to exercise when faced with threats. In our research, the PMT especially inspired the development of a risk perception monitoring tool to identify and describe the various factors associated with individuals' intention to adopt protective measures.

This research is based on a large-scale quantitative survey (N=1.033). Data have been collected in the first quarter of 2015 by a market research company and are representative of the overall Belgian population.

A segmentation of the Belgian internet users has been constructed based on four factors pertaining to online activity and security: (1) frequency of internet use; (2) variety of internet use; (3) variety of security measures; and (4) perceived safety of the internet. Our segmentation distinguishes four profiles: (1) ***The conscious internet users*** (32% of the sample, Profile 1). Respondents belonging to this profile are young and highly-educated citizens who make frequent use of the internet. They take no risks and employ multiple security measures to protect them against cybercrime threats; (2) ***The overly confident internet users*** (13,5% of the sample, Profile 2). Respondents belonging to this profile are older and low-educated individuals who are frequently online. They have great confidence in the internet and only take minimal security measures to protect them against cybercrime threats; (3) ***The inexperienced internet users*** (35,5% of the sample, Profile 3). Respondents belonging to this profile tend to be older and less educated. They are not frequent users of the internet. They are not ICT literate, have little trust, would rather reduce their online time instead of taking security measures and are poorly protected; (4) ***The resolved internet users*** (19,1% of the sample, Profile 4). Respondents belonging to this profile are older and rather low educated individuals, who make often use of the internet. They take internet security seriously and seek for protection. They also have the confidence to engage in online activities that are considered unsafe by other people.

In terms of user attitudes, it is important to learn more about how people perceive the safety of online activities. Based on our analysis, we can conclude that internet activities such as 'information retrieval', 'news consumption', 'e-mail' and 'electronic banking' are considered to be the safest activities. Although quite some respondents have trust in online banking, a number of respondents also have doubts about this. Especially 'downloading' and 'social media' are online activities our respondents consider to be unsafe. More in general, we can conclude from our analysis that there exists a lot of distrust in the online environment.

This reports also focuses on cybercrime victimization. More specifically, we have analyzed whether or not our respondents have been the victims of different types of cybercrime. Based on our data we can conclude most of the respondents had to deal with viruses. Corporate surveillance is also an aspect that is mentioned a lot, although we have to add that for this category also a large group is undefined whether they have been victims or not. Scams and hacking seem to be the cybercrime types of which our respondents have been least the victims. In the report we do not only provide a general overview, we also go more in detail for each type of cybercrime. More in particular, the occurrence, the perceived severity, and whether or not the victims have reported the encounter of the cybercrime, are aspects we present detailed information about.

Another part of the report has paid attention to the financial impact of cybercrime. For this aspect, we have asked the respondents to estimate the costs that have occurred because of being the victim of different types of cybercrime. Based on our analysis we can conclude that especially scams and hacking seems to result in larger costs. For the categories governmental and corporate surveillance, but also unwanted content and/or behavior, the respondents find it more difficult to make an estimation of this.

In terms of risk perception, we made use of the Protection Motivation Theory (PMT) to predict the intention that internet users would take security measures. In this context we have performed regression models to determine to what extent the PMT variables are associated with intention to use internet security measures, according to the four profiles of internet users. Based on the analysis, especially the respondents belonging to Profile 2 – The overly confident internet users and Profile 3 – the inexperienced internet users seem to be the most vulnerable groups. They not only have limited knowledge about the internet and the online risks, they are also least informed about internet risks and how to avoid them.

A final part of the report focuses on risk communication. In this context we distinguish between target groups on the one hand and topics and content on the other hand. As indicated above, the respondents belonging to Profile 2 and 3 are most vulnerable and therefore deserve particular attention in cybercrime awareness campaigns. In terms of how to approach these groups, we stress a balance needs to be found between on the one hand informing citizens about the potential dangers that exist on the internet, while on the other hand giving them confidence to take measures on their own behalf and inform them about the effectiveness of taking internet security measures.

INTRODUCTION

Late 2005, a watershed event took place in the worldwide penetration of information and communication technology: the number of computer users with internet access crossed the one billion mark (Anderson & Agarwal, 2010). Ten years later, this number has more than tripled, with an estimated 3,1 billion people being connected to the World Wide Web (Internetlivestats.com, 2015). Belgium is definitely not lacking behind this digitalization trend, with 83% of all Belgian households having an internet connection at their disposal in 2014 (SPF Economy, 2015). When children are part of these households, more than nine in ten (94%) report being connected to the internet. Digimeter 2014, which measures digital media trends in Flanders, even found a staggering 92,4% of all people, aged 15 or older, being active online (Digimeter, 2014). From these figures we can conclude that the Belgian population is exposed to the risks and threats that are inherent to the online environment.

'Cybercrime', commonly used as an umbrella term for different threats in the cyber world, appears to be on the rise. CERT.be, the federal cyber emergency response team run by Belnet (Belgian national research network), has recorded more than twice as many cyber incidents in 2014 than it did the year before, and even seven times as many as in 2010. In its press release (Cert.be, 03/09/2015), the organization further stated that these incidents became more and more complex. The higher victimization rate is partly explained by an increased visibility of and awareness around the organization, but the overall trend is not to be denied. Given the fact that only a small part of the incidents is reported, one can only imagine how much of the iceberg we are truly witnessing (Datanews, 2015).

Cybercrime is characterized by a wide variety of perpetrators and victims. Besides the attacks that are accounted for in current work (civilians as subjects of victimization), private and public companies are also targeted frequently. Several years ago, the French-Dutch company Gemalto, world's largest producer of SIM cards, became victim of a large-scale hacking by American security agency NSA and their British counterpart GCHQ (De Tijd, 2015). As a result of this, mobile traffic could be deciphered and millions of users eavesdropped. The revelations of Edward Snowden in 2013 created a global awareness of this problem, illustrating the increase of both governmental and corporate surveillance on citizens worldwide.

Simultaneously, the public sector is lacking behind when it comes to securing its electronic services against cyber-attacks (DeMorgen, 2015). SSL Labs-tests revealed outdated versions of the SSL encryption protocol on governmental sites, leaving user data susceptible for information breaches, and thus many people vulnerable to malicious third parties. Only recently, the ambition is formulated to create a fourth Belgian army division, which will deal in a responsive and proactive manner with cyber-attacks. "Our safety nowadays relies more than ever on the safety of data traffic", underpins Minister of Defence Steven Vandeput the decision (DeRedactie.be, 2015).

However, the count of individual attacks in itself says little about the cost and impact of cybercrime, since it is quite easy to obtain large numbers (Singer & Friedman, 2014). Indeed, looking at the impact caused by cybercrime is a better way to gain insight in this complex phenomenon. In scientific literature, increased attention is being focused on end-users or citizens, as victims of cybercrime. Unlike employees in a work setting, these internet users are not subject to training or protected by a technical staff (Anderson & Agarwal, 2010). Therefore they can be more vulnerable and thus deserve to be the topic of scholarly research.

The aim of the research presented within this report is fourfold:

1. To identify and clearly define **profiles for risk communication efforts**, based on the online activity of the Belgian citizen and the security measures he/she undertakes;
2. To **deepen the understanding of the different sorts of cybercrimes**, their occurrence and how they are handled with;
3. To develop a **risk perception monitoring tool to identify and describe factors associated with the public's intention to adopt protective measures;**
4. To formulate **recommendations considering risk communication efforts related to cybercrime.**

THEORETICAL PERSPECTIVES

1 Cybercrime: Definition and scope

Although the term 'cybercrime' is now widely used in scientific literature, a first problem encountered in measuring cybercrime is that there is no commonly-agreed upon definition of the term. Cybercrime has become a common term and its usage tends to generalise just about any illegal activity within the internet environment. This lack of definitional clarity is problematic as it impacts every facet of e-crime investigation and the reporting process.

Within the BCC project, the agreed upon definition of 'cybercrime' reads as follows (WP1):

*"**Cybercrime** comprises all computer-mediated activities, committed over electronic communication networks and information systems in an electronic environment, which are either illegal or considered illicit by certain parties and which can be conducted through all global electronic networks and media. These activities affect society as a whole due to their cost for and impact on individuals, industry and the government. They are directed against the confidentiality, integrity and availability of automated processes/resources and focused on interfering with or affecting the operation of computer systems/systems that maintain automated processes."*

The present general definition points out the complexity of the matter at hand. Given the practical aim of the project and the aforementioned problems regarding semantics, a categorization of the considered forms of cybercrime imposes itself. These forms in which cybercrime manifests itself, are based on categories derived from scientific literature (in this regard it is important to mention the typologies that were formulated by Holt and Bossler, 2014, and Anderson et al., 2013), on practice (Veiligheidsmonitor, 2013), and on expert consultations. They include:

1. **Viruses** (e.g. malware, botnets);
2. **Scams** (e.g. in online banking);
3. **Hacking** (e.g. unlawful access, identity theft);
4. **Governmental surveillance** (monitoring/data collection of citizens by the government);
5. **Corporate surveillance** (monitoring/data collection of citizens by companies);
6. **Unwanted content and/or behavior** (e.g. sexual or racist content, cyberbullying, stalking).

2 Protection Motivation Theory

The theoretical model underpinning the research presented in this report is based on the Protection Motivation Theory (PMT; Rogers, 1975), and was applied to cybercrime and protective measures in general. PMT has proven to be a useful theoretical foundation for understanding the process that individuals go through in deciding which security behaviors to exercise when faced with threats. It exposes the determinants or drivers of either adaptive or maladaptive coping with security threats. In respect of this particular study, protective measures like installing anti-virus software or changing privacy settings can be considered adaptive coping. Reducing internet use or avoiding/stopping certain activities can be labelled as maladaptive coping mechanisms. As such, PMT is used here to develop a risk perception monitoring tool to identify and describe the various factors associated with individuals' intention to adopt protective measures.

The perceived threat is composed of two dimensions: perceived susceptibility to the threat (i.e. the degree to which one feels at risk for experiencing the threat) and perceived severity of the threat (i.e. the magnitude of harm expected from the threat). Perceived efficacy or coping appraisal also is composed of two dimensions: perceived self-efficacy (i.e. one's beliefs about his or her ability to perform the recommended response) and perceived response efficacy (i.e. one's beliefs about whether the recommended response works in averting the threat). Prior victimization can be considered a source of information that directs subsequent (in)action (Riek et al., 2014). Whether or not people have become a victim of cybercrime could influence both their appraisal of the threats and adjoined coping abilities. These three variables constitute the attitude towards security-related behavior. On its turn, the intention to perform this behavior is determined by attitude and subjective norm. This latter concept can be described as the perceived social pressure to engage or not in a certain behavior.

Besides explaining attitudes, behavioral intentions and actual behavior, PMT has proven to be valuable in explaining when and why fear appeals work in communicating about the risks of contemporary society (Witte & Allen, 2000). A highly perceived threat and efficacy will result in a better acceptance of the message; just as fear appeals and high-efficacy messages motivate adaptive actions aimed at controlling the danger (e.g. message acceptance) instead of maladaptive fear control actions (e.g. defensive avoidance). However, a significant difference between PMT and fear appeal theories is the cognitive focus of PMT and the rather trivial role that is accorded to fear.

Theoretical model

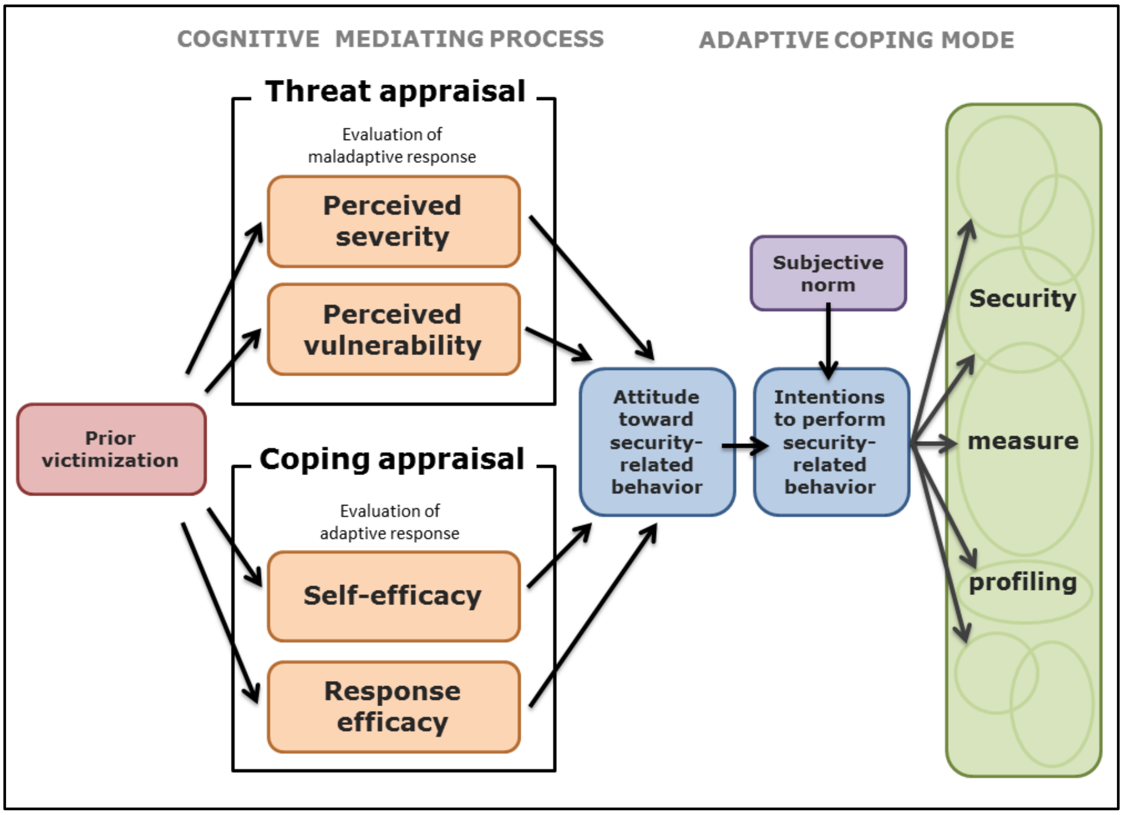


Figure 1 – Theoretical model

3 Internet security profiling

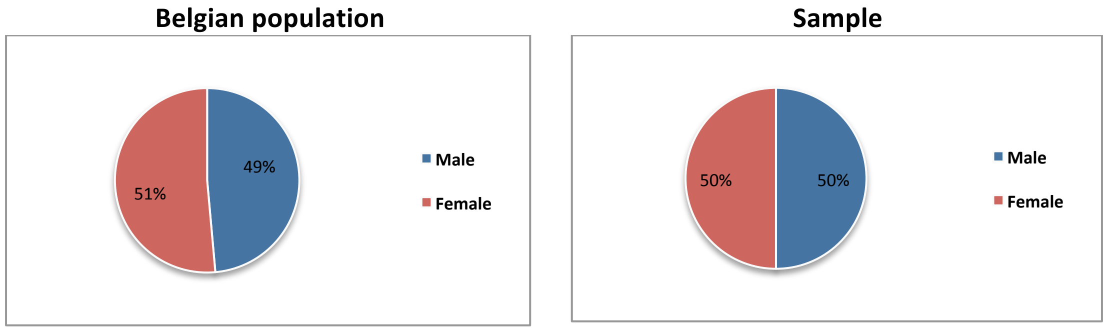
In this study, we aimed for identifying distinctive types of internet users' orientation towards security in the context of their online activities. While cyber security is a high-priority activity for security experts and researchers, citizens conduct it in the context of their daily lives, as a socially accountable and resource-limited activity (Rughiniş & Rughiniş, 2014). Classification analysis is a productive tool for understanding these security orientations through survey data and for informing public interventions. The obtained empirical diversity of user profiles could yield important insights for researchers, practitioners and policy makers.

METHODOLOGY

1 Sample

The research presented in this report is based on large-scale quantitative research with a representative sample of the Belgian population. The quota for representativeness are based on the FPS Economy statistics of 2014 and include age, residence and gender. A comparison of the Belgian adult population and the sample characteristics based on these criteria, is shown in Figures 2, 3 and 4. Overall, our obtained sample can be considered representative for the active Belgian internet population in terms of these quota, and therefore there was no need of weighing of the obtained data.

Distribution by gender



Belgian population

Sample

Figure 2 – Gender distribution within the adult Belgian population (FPS Economy, 2014) versus the sample (N=1.036)

Our sample consists of an equal number of women and men (50,0%).

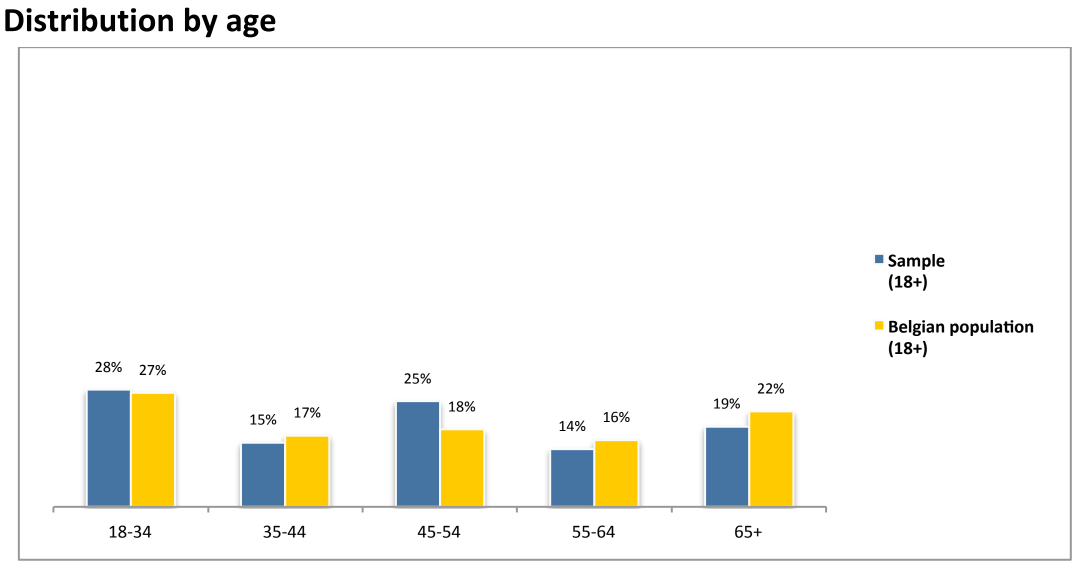


Figure 3 – Age distribution within the adult Belgian population (FPS Economy, 2014) and the sample (N=1.036)

The minimum age to participate in the survey was 18 years old. The average respondent is 47 years old, with a minimum of 18 and a maximum of 87 years (*M* = 47,45, *SD* = 15,75).

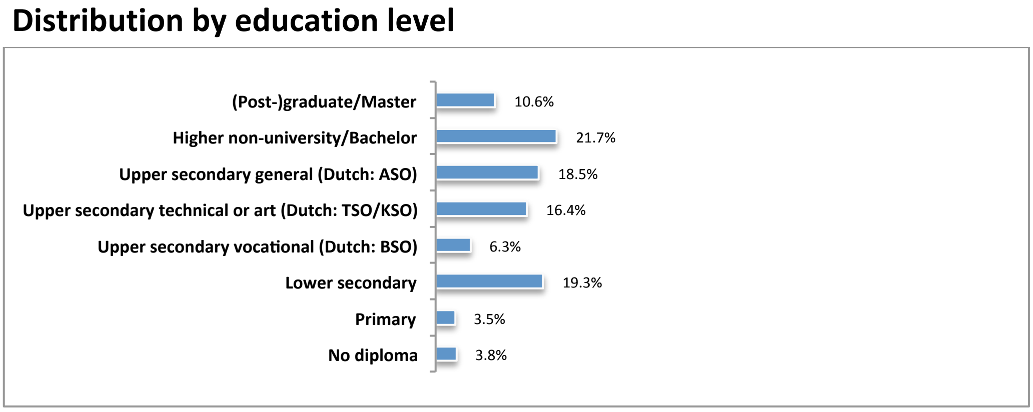


Figure 4 – Education level distribution within the sample (N=1.033)

Most of the people in our sample attended at least secondary school, whereas 7,3% only completed primary education or had no degree at all (see Figure 6). 32,3% has a higher degree (higher non-university, bachelor, master or post-university).

Distribution by employment situation

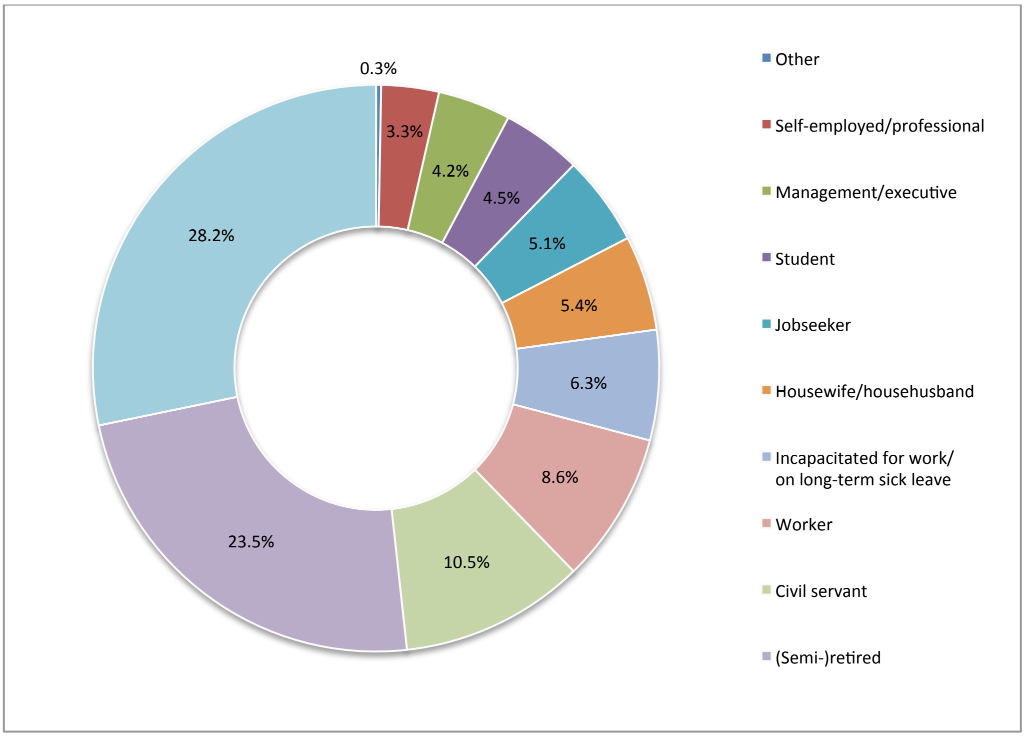


Figure 5 – Employment situation distribution within the sample (N=1.036)

Our sample is further characterized by a majority that is professionally active as a clerk or that is (semi-)retired: combined they add up to more than 50% of our sample (see Figure 5). Of the three people that gave up another profession then the ones prelisted, two indicated that they were voluntary workers, and one person indicated that she is a widow.

Distribution by family situation

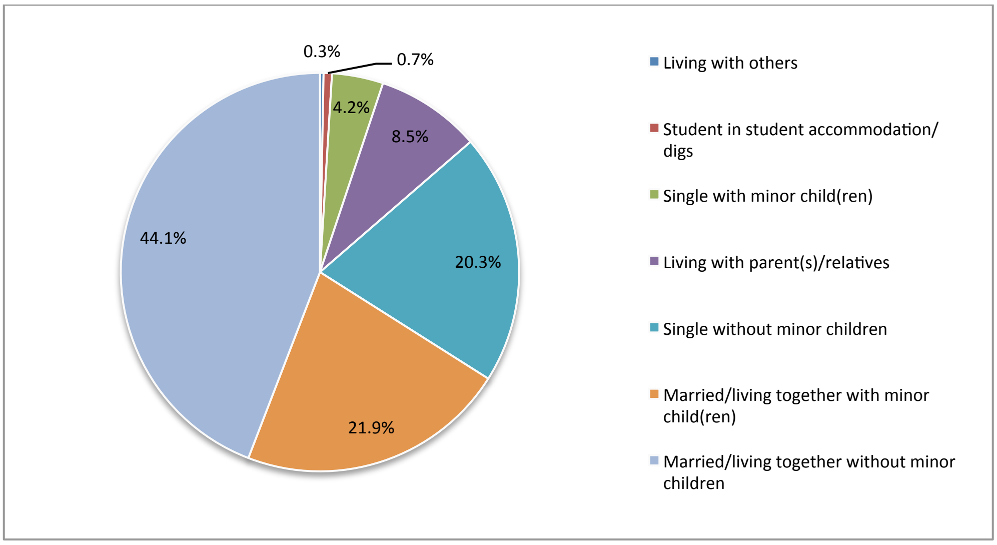


Figure 6 – Family situation distribution within the sample (N=1.033)

Within our sample, the vast majority of the people live together with their partner or spouse without any minor children (44,1%), followed by those who do so with minor children (21,9%, see Figure 7).

Distribution by residence

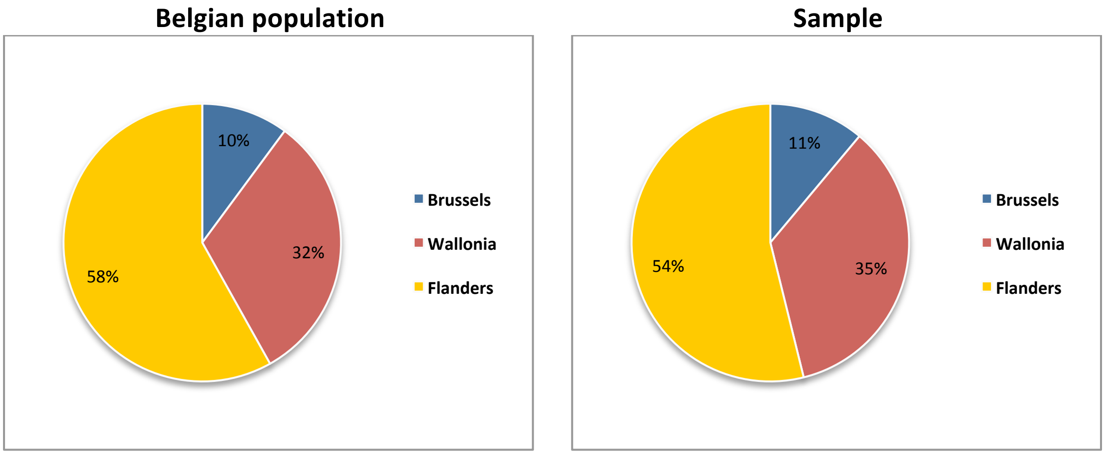


Figure 7 – Residence distribution within the adult Belgian population (FPS Economy, 2014) versus the sample (N=1.036)

More than half of the respondents (53,9%) reside in Flanders, more than a third (35,0%) in Wallonia, and a smaller amount (11,1%) in Brussels.

2 Measures

For a detailed description of the measures that have been used in our research, we refer to the appendix (p. 88).

2.1 Online activity

Various measures are used to capture the online activity of the respondent. These are based on questionnaires of the Digimeter (2014), ICT statistics of Belgian households by FPS Economy (2013) and the Eurobarometer (2013), and include the variables that deal with having devices at one's disposal that are connected to the internet, the frequency of internet use and online activities. The respondents' online activity can be seen as a proxy for the perceived advantages or possibilities the internet has to offer for them.

> Question: "*How often do you use the internet during a typical week?"*
> *(at home during work days/at home during the weekend /at work)*
> *Never – Less than weekly – Less than daily – Less than 1 hour per day –*
> *Between 1 and 3 hours per day – More than 3 hours per day*

2.2 Being informed

A core issue for describing citizens' security behaviors refers to risk awareness. Therefore, a measure for being informed about internet related risks, and how to tackle/avoid them, was included. The formulation of the two items making up this construct is in part based on the Eurobarometer (2013).

> Example item: "*I feel adequately informed about how to avoid the risks of the internet."*
> *Five point Likert scale: Totally disagree – Totally agree*

2.3 Confidence in the safety of the internet

Internet users' trust or general confidence in the safety of the internet is taken into account since trust is seen as the counterpart of perceived risk (Riek et al., 2014). The variable is measured in analogy with de Jonge et al. (2007). In this work, the confidence in food safety is assessed on the basis of two dimensions: 'optimism' and 'pessimism'. Four of the original seven items were retained and applied to the safety of the internet, forming a unidimensional instrument measuring confidence or trust in the safety of the internet. The deleted three items obtained the lowest factor loadings when testing the instrument's dimensional structure (de Jonge et al., 2007), and proved to be the least understood items during pretesting.

> Example item: "*I am concerned about internet safety."*
> *Five point Likert scale: Totally disagree – Totally agree*

2.4 Safety of internet-related activities

Again in analogy with de Jonge et al. (2007), a selection of internet-related activities can be judged in terms of their safety. Respondents can indicate 'I don't know (it)' when they are not familiar with the activity in question or cannot assess its safety.

Question: "*How safe do you think these activities are in general?"*
Five point Likert scale: Not safe at all – Very safe

2.5 Severity and probability of cybercrime forms

In traditional criminology literature, fear of crime is considered multidimensional in nature, consisting of two distinct components (Riek et al., 2014). First, the rather rational risk perception, which is often operationalized as a product of the probability of victimization and the severity of the crime. Second, fear is seen as a rather emotional feeling of being unsafe. In our research, we focus on the perceived risk, as we do not intend to clarify the relationship between both components. In accordance to the work of Greenfield and Paoli (2013), in which harms (severity x incidence) are considered as a basis for prioritizing criminal activities, perceived risk (severity x probability) can guide a similar approach.

Question: "*In your opinion, how serious are the following phenomena?"*
Five point Likert scale: Not serious at all – Very serious

Question: "*How likely is it that you will become a victim of the following phenomena?"*
Five point Likert scale: Very unlikely – Very likely

2.6 Cybercrime victimization

Questions pertaining to cybercrime victimization and also the more in-depth questioning when victimization did occur in the past twelve months are based on the *Veiligheidsmonitor*, a yearly public safety monitoring tool used in the Netherlands.

Question: "*Have you, or anyone else in your family, experienced any of the following situations in the past 12 months?"*
Yes, myself – Yes, someone else in my family – Yes, both me and someone else in my family (e.g. shared computer) – I suppose so – No – I don't know

2.7 Safety measures

In defining our six broad categories of protective measures, we were inspired by the STOP. THINK. CONNECT. recommendations, as formulated on the Stay Safe Online website by the National Cyber Security Alliance (Staysafeonline.org, 2015). However, in predicting protective measures or user protection profiles, we chose security precautions that require a deliberate and voluntary (in)action. Having a firewall up and running or keeping your software up-to-date for example, are mostly automated processes nowadays, and is thus not included.

Question: "*Do you take one or more of the following security measures to protect yourself or your family against such incidents?*

The six security measure categories include:

- Reducing internet use (e.g. less downloading behavior, reducing the use of social media);
- Avoiding or stopping certain activities (e.g. ignoring certain mails, refraining from online banking);
- Changing settings (e.g. adjusting privacy settings on social media, spam filter, changing passwords);
- Creating a backup;
- Installing software (paying);
- Installing software (non-paying).

2.8 Theoretical model

All used measures pertaining to the cognitive mediating process within our theoretical model were adapted from previous literature, as validated measures exist for all the independent variables (cfr. Crossler & Bélanger, 2014). PMT researchers developed the Risk Behavior Diagnosis (RBD) scale, which encompasses severity of the threat, susceptibility to the threat, self-efficacy, and response efficacy (Witte, 1996). Regarding self-efficacy, it was important to follow the recommendation by Marakas et al. (2007) to adapt the self-efficacy measure to fit the context being studied. Therefore, we based ourselves on the instrument developed by Anderson & Agarwal (2010) for the measurement of this construct. These authors further served as a very useful source for measuring the attitudes towards and intentions to perform security-related behavior. Our PMT instrument's wording and general face validity was further screened by an expert in the field.

Example item **perceived severity**: "*I believe that cybercrime is severe.*"
Example item **perceived vulnerability**: *"It is likely that I will be a victim of cybercrime."*
Example item **self-efficacy**: "*Taking the necessary security measures is easy.*"
Example item **response efficacy**: "*By taking protective measures, I can prevent cybercrime.*"
Example item **attitude towards security-related behavior**: "*Taking security measures is a good idea.*"
Example item **intentions to perform security-related behavior**: "*I am certain that I will take (more) security measures.*"
Example item **subjective norm**: "*My friends think that I should protect myself against cybercrime.*"
Five point Likert scale: Totally disagree – Totally agree

2.9 Socio-demographic variables

The included socio-demographic variables are based on the questionnaires of Digimeter (2014) and FPS Economy (2014), and include gender, age, residence, professional situation, education level and family situation.

3 Procedure

In order to answer the above-mentioned research questions, the research group iMinds-MICT launched an online survey in the first quarter of 2015. The participants were recruited with the help of a professional market research agency (iVOX). An URL to the questionnaire was made available by the research team and sent to 6.670 panel members by e-mail. Incentives in form of gift vouchers were handed out to a number of randomly picked participants. Three weeks after launching, the survey was at least partly filled out by 1.289 end-users from a wide range of demographic and socio-economic backgrounds, yielding a response rate of 19,33%. A total number of 1.033 participants filled out the survey completely (15,49%), which took them on average 15 minutes (trimmed mean).

In what follows, distinct clusters of respondents are firstly identified, based on their frequency and variety of online activity, variety of security behaviors and perceived safety of internet-related activities. In order to reduce the number of variables to include in this cluster analysis, multiple factor analyses are performed. A factor analysis is the method by choice to reduce the data and detect underlying structures. Secondly, each cybercrime category is described separately. This allows for a better insight into cybercrime victimisation in Belgium and how victims handle this. These statistics are exclusively descriptive and explorative of nature. Source of this data was an open question included for each cybercrime category, asking to briefly describe what exactly happened the last time the participant encountered such a crime type. This question contributes to the uniqueness of the current study, allowing for a better interpretation of the data and a more in-depth, qualitative analysis of what exactly happened. In a third section we develop a risk perception monitoring tool to identify and describe factors associated with the public's intention to adopt protective measures. The Protection Motivation Theory (PMT) serves here as a theoretical backbone. Finally, based on all previous findings, we develop recommendations pertaining to risk communication campaigns.

SURVEY RESULTS

1 Profiling the Belgian internet user

In order to profile the Belgian internet user, results are first analysed for the whole sample. Based on their online activity and the security measures they take, the respondents are consequently profiled in four different and distinguished categories. These obtained profiles serve as a constant throughout this research report. The way of reporting the results follows the same pattern in each section: the characteristic is first described for the entire population, after which we provide more in-depth results comparing subgroups, when cross tabulations yield significant chi-square statistics ("distribution tests"). Note that the subgroup percentages are only mentioned when they indicate significant differences between these subgroups (threshold for standardized residuals: +/- 2).

1.1 Online activity

Our sample is characterized by a frequent use of internet at home, but a rather moderate to no use of the internet at work (see Figure 8). Most hours online are clearly spent at home during leisure time.

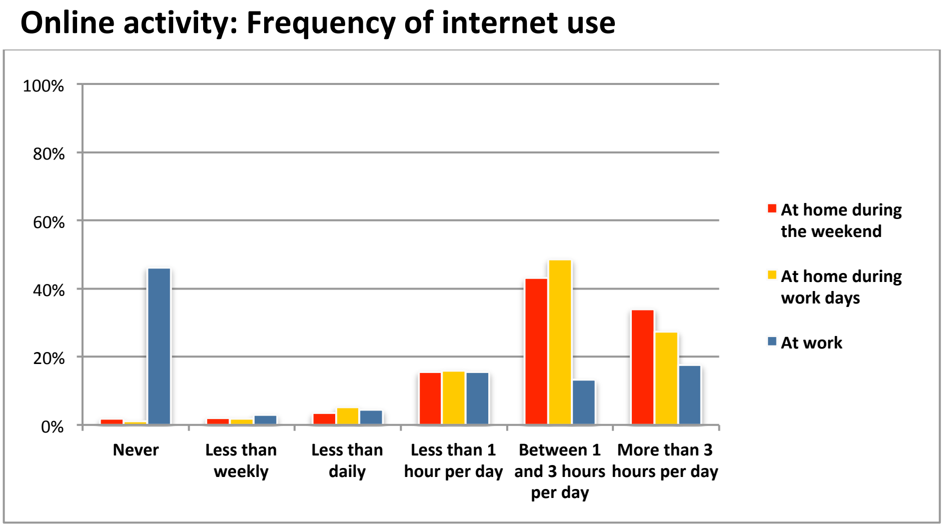


Figure 8: How often do you use the internet during a typical week? (N=1.229)

The low frequency of internet use at work is mostly explained by people of *65 years or older*: 98,5% of this age category never accesses the internet in a professional context (χ^2 (20, N=1.036) = 400,59, p<.001). Not surprisingly, the main reason for this finding is their professional status: a large majority (95,9%) of these people is *(semi-)retired* (χ^2 (40, N=1.034) = 1.047,95, p<.001). Perhaps contrary to what we might have assumed, it has less to do with the blue/white collar divide. Of those that never use the internet in a professional context, only 8,8% has a *workers'* statute, while 10,1% is *housewife or househusband*, 11,3% is *incapacitated for work or on long-term sick leave*, and 50,1% is *(semi-) retired* (χ² (50, N=1.034) = 678,73, p<.001). Most people active in the labour market spend a considerable amount of time online during working hours since the digitalization of the workspace.

A large majority (87,5%) of the people that never use the internet at home during work days, lives in *Wallonia* (χ² (10, N=1.036) = 21,13, p<.05, caveat: expected count < 5 (2,8)), and half of them belongs to the *age category 35-44* (χ² (20, N=1.036) = 38,54, p<.01). On the contrary, 35,1% of those that spend more than three hours online at home during a working day, is *younger than 35 years old*. More than half of respondents (52,8%) that dropped out of school after *primary education*, spend daily more than three hours on the internet at home during working days (χ² (35, N=1.033) = 66,03, p<.01). Likewise, 41,5% of those that achieved *upper secondary vocational (BSO)* as their highest education, spend the maximum amount of time online when at home during a typical working day. *(Post-)graduates or Masters* contrast with these groups, since they make up only 5,8% of those who spend so much time online when not at work during a work day. Almost a fifth (18,6%) of the *single parents* do not connect on a daily basis with the internet at home, presumably because they lack the time to do so during the work week (χ² (30, N=1.033) = 75,58, p<.001). Likewise, of those *married or living together with minor child(ren)*, only 18,1% spend more than three hours online at home during a work day.

Compared with respondents *older than 64 years old*, more than double the number of people *younger than 35 years old* spend more than three hours online during a typical day in the weekend (21,9% versus 44,2%, χ² (20, N=1.036) = 55,48, p<.001). *(Semi-)retired* people add up to 64,3% of those that never go online during the weekend (χ² (50, N=1.034) = 127,69, p<.001). Almost three quarter (70,2%) of *students* spend more than three hours online during weekend days. 55,4% of those that achieved *upper secondary vocational (BSO)* as their highest education, spend more than three hours per day in the weekend on the internet, whereas only 20,0% of those with a *(post-) graduate or Master's degree* do so (χ² (35, N=1.033) = 75,50, p<.001). However, this does not mean that the latter do not spend a considerable amount of time online during the weekends: 55,5% of *university graduates* is daily online between one and three hours. Of the people that use the internet less than daily during weekends, a majority (38,9%) has a *higher non-university or Bachelor's degree*.

Activities like information retrieval, consulting news sites, reading/sending e-mail, electronic banking, being active on social media platforms, and to a lesser degree purchasing and/or selling goods on the internet, are the most popular internet activities (see Figure 9). These activities are all mostly being done on only one of the prelisted devices, with percentages ranging from 66,4% for online banking, to 31,8% for social media. For the latter category, we also notice quite some respondents (25,6%) who do this on two or more devices.

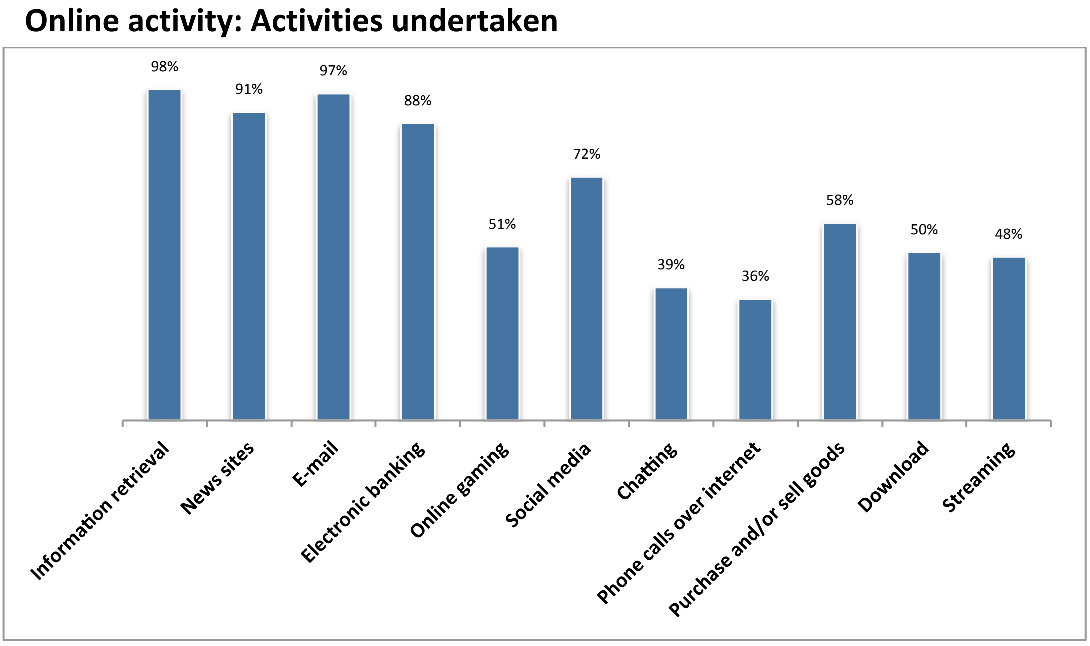


Figure 9: Which of the following activities have you done in the past month using your device(s)? (N=1186)

In order to reduce the number of variables to include in our cluster analysis, a factor analysis was performed on the data (see Table 1). Note that the sum variables, that add up to a total number of different devices on which one has practiced the activity in the past month, served as input for these factor analyses. Another possibility for performing this analysis is with binary variables: has the respondent done the activity during the past month on one of the prelisted devices, regardless of the number of devices on which he/she has done it? Both approaches yield similar results. However, to include the number of devices in our analysis (which can also be seen as a proxy for the frequency of internet use), we have decided to continue with the sum variables.

This analysis yielded a clear distinction between two groups of activities. On the one hand, people involve in more traditional online activities like information or news retrieval, e-mail management, online banking or, to a lesser degree, e-commerce. These can be considered as more traditional, passive online activities (α=.83, having ‘purchase and/or sell goods’ deleted). ‘Passive’ refers in this context to those activities that are mostly unilateral and characterized by a low degree of social interaction. Not surprisingly, these activities are practiced the most (with the exception of visiting social media platforms, which is also quite popular, see Figure 9). On the other hand, activities where active, direct verbal or non-verbal communication is key, like social media, online gaming, chatting, or VoIP (Voice over IP) services, can be distinguished (α=.77, having ‘streaming’ deleted). E-mail is considered a more traditional activity, since this communication tool does not require immediate response, and has been around for quite a while now. E-commerce, streaming and downloading (to a lesser extent) float in between both ends of this continuum and achieve the lowest factor loadings. A possible explanation for this finding is that e-commerce – considered a traditional activity – often does involve direct communication, and downloading and streaming – considered a social activity – can be considered as manifestations of passive online content sharing.

Table 1: *Rotated factor loadings of online activity sum variables*

	Loadings	
	Traditional activities	**Social activities**
Information retrieval	**.80**	.30
News sites	**.77**	
E-mail	**.78**	
Electronic banking	**.72**	
Online gaming		**.67**
Social media		**.65**
Chatting		**.78**
Phone calls over internet		**.64**
Purchase and/or sell goods	.55	.33
Download	.37	**.60**
Streaming	.47	.58
Initial eigenvalue	5,11	1,09
Variance (%)	46,46	9,91
Rotated variance (%)	29,79	26,58

Rotated Component Matrix
Extraction method: PCA
Rotation method: Varimax with Kaiser normalization
Bartlett's Test of Sphericity: .00 sig.
Two components explain 56,37% of the variance (loss of 43,63%).
Factor loadings < .30 are not withhold.

People residing in *Brussels* seem to involve a lot in online social activities, compared to other regions. Quite a few of them (28,7% or almost a third) participated in all five prelisted social activities (*streaming* excluded for reasons mentioned above) in the last month, roughly double the number of the people from *Flanders* (14,3%) or *Wallonia* (17,6%, χ^2 (10, N=1.036) = 22,09, p<.05). As expected, younger respondents engage a lot more in online social activities than older people do: of the people that involved in four or five distinct social activities, respectively 44,1% and 55,9% belong to the *18-34 age group*, compared to 21,4% and 5,7% that is *older than 54 years old* (χ^2 (20, N=1.036) = 203,17, p<.001). A majority of the respondents in the category *18-34 years old* (34,7%) indicated they did all five social activities on their device(s) in the past month. Not surprisingly, the same (48,9%) can be said about *students* (χ^2 (50, N=1.034) = 204,75, p<.001), since all *students* (100,0%) belong to this age group (χ^2 (40, N=1.034) = 1.047,95, p<.001).

Most people (40,0%) that achieved *upper secondary vocational education (BSO)* as their highest educational level, engaged in all five online social activities in the last month (χ^2 (35, N=1.033) = 77,21, p<.001). Likewise, most *workers* (34,8%) have participated in a maximum number of online social activities (χ^2 (50, N=1.034) = 204,75, p<.001). Half the *(semi-)retired* people (50,2%) have done no or only one social activity during the past month. People that are *married or living together, and have minor children*, tend to engage more in online social activities: they make up 32,2% of the people that achieve a maximum number of social activities (χ^2 (30, N=1.033) = 115,95, p<.001). This is in contrast to *couples without children*, of which only 11,2% indicated they did all five online social activities. This could be the influence of the children that connects their parent(s) with technology, although we do not see this effect occurring with *single parents (mom or dad)*. Respondents that *live with their parent(s) or relatives* are also socially active online (33,0% checked off all five activities), which should come as no surprise since 84,1% of them belongs to the *youngest age category* (*18-34*, χ^2 (24, N=1.033) = 409,60, p<.001).

When looking at how these activities are perceived in terms of their safety, the traditional activities are roughly seen as safer than the social activities, with the notable exception of purchasing and/or selling goods online (see Figure 10). It seems that when direct social interaction is involved, people fear malicious intentions of their counterpart(s). Downloading and being active on social media platforms is considered to be the most risky activities of those prelisted, with respectively 47,0% and 45,9% of our sample having marked these activities as not safe or not safe at all. On the other hand, consulting news sites and retrieving information online are perceived as the safest activities, with respectively 62,5% and 56,4% of the sample labelling them as safe or very safe. Making phone calls over the internet and online gaming are the least understood/familiar technologies, we learned from respectively 21,3% and 21,0% of our sample, indicating that they do not know the activity or they cannot properly assess its safety. A three-item scale (Cronbach's Alpha = 0,82), measuring the overall confidence in the safety of the internet shows that it is surely not exaggerated to state that the respondents seem to have little trust in the safety of the internet (*M*= 2,73, *SD*= 0,76).

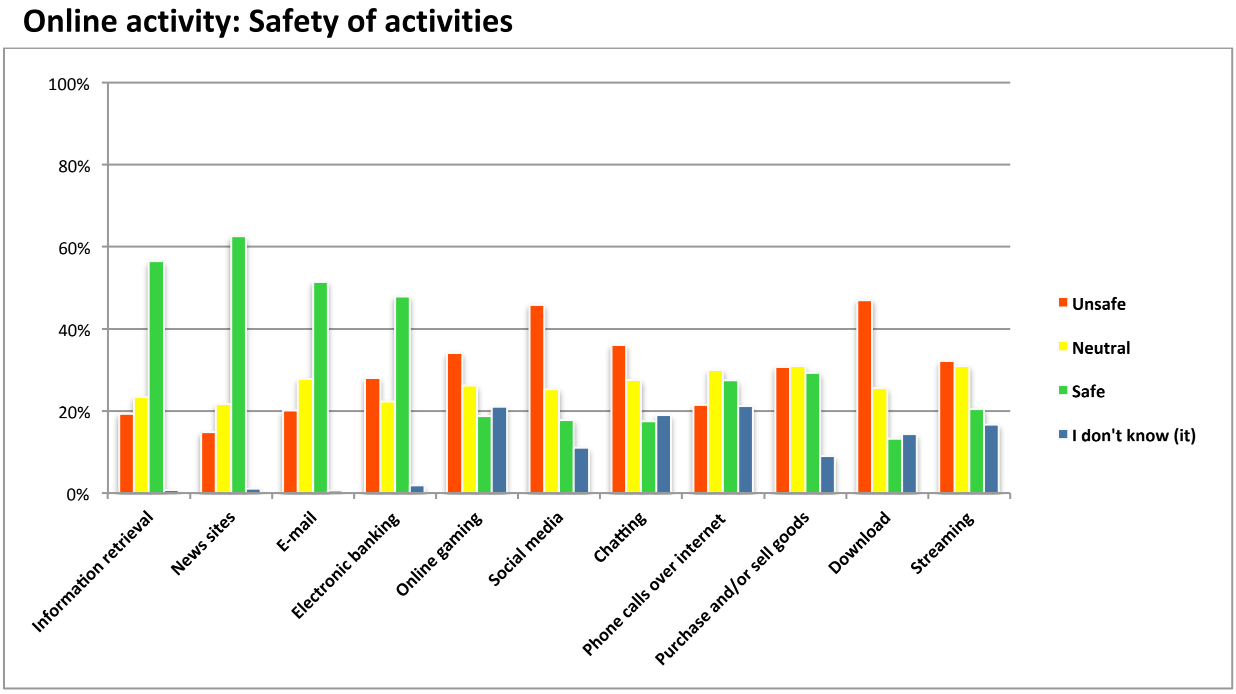


Figure 10: How safe do you think these activities are in general? Respectively 'Not safe and 'Not safe at all' combined into 'Unsafe', and 'Safe' and 'Very safe' into 'Safe'. (N=1129)

1.2 Security behavior

The protective measures people take form the second angle on which the cluster analysis is based. Almost all (98,6%) Belgian citizens take a diversity of protective measures, in order to secure themselves and their online experience from different types of cybercrime. These security behaviors range from having software installed (whether or not paid), over creating a backup and adjusting settings (e.g. privacy settings on social media, spam filter or changing passwords), to reducing internet use (e.g. downloading less or using less social media) and refraining from certain online activities (e.g. ignoring certain e-mails or refraining from online banking). Most people (54,4%) have free software installed on their device, followed closely by half the people (49,6%) that avoid or stop certain activities (see Figure 11). This finding supports the statement that cybercrime causes many indirect losses or opportunity costs in the form of maladaptive coping behavior (Anderson at al., 2013; Riek et al., 2014). This can be understood as a reduced uptake of electronic services by citizens, resulting from a decreased trust in the online environment.

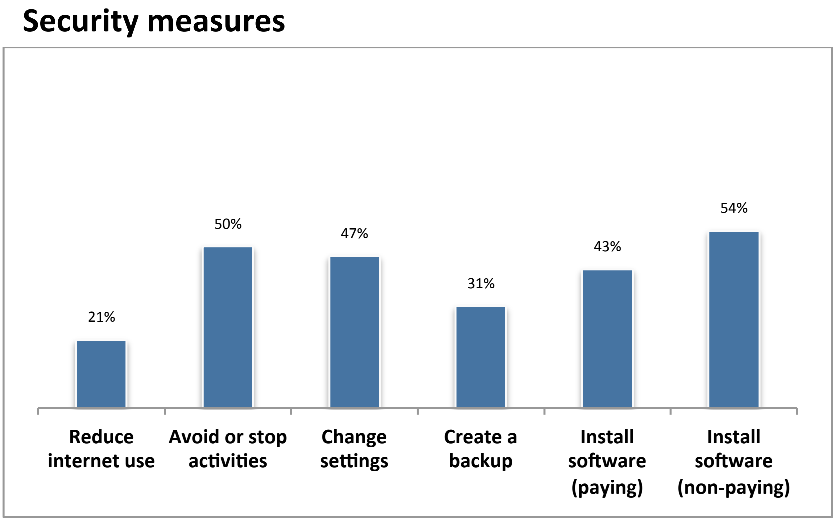


Figure 11: Do you take one or more of these security measures to protect yourself or your family against cybercrime? (N=1083)

The respondents are most likely to *install software* as a protection against **viruses** (see Table 2). More than half the number (50,4%) of internet users does so *without paying for the software*. *Avoiding or stopping certain internet-related activities* is the preferred action to take against **scams**, we learn from almost one third (30,6%) of the respondents. Again almost one out of three respondents protect their online experience from being **hacked** (28,0%), **government surveillance** (27,2%) or **corporate surveillance** (29,8%), or ***witnessing unwanted content and/or behavior*** (26,8%), by *changing the settings* of their device, software or web pages. Since *creating a back-up* is least effective against **being the subject of surveillance** or **encountering unwanted content/behavior online**, this protective measure is not often in place for these threats. The Belgian internet user is least likely to *reduce the time spent online* in order to avoid most of the predefined threats.

Table 2: *Frequency table of security measures taken against internet threats*

	Reduce internet use	Avoid or stop certain activities	Change settings	Creating a back-up	Install software (paying)	Install software (non-paying)
Viruses	**6,19%**	27,15%	22,62%	26,59%	**39,89%**	**50,42%**
Scams	**6,93%**	**30,56%**	24,10%	**9,60%**	24,65%	**26,78%**
Hacking	**8,68%**	**27,61%**	**27,98%**	**10,53%**	26,32%	31,02%
Governmental surveillance	**12,28%**	21,14%	**27,15%**	**7,85%**	17,17%	**23,55%**
Corporate surveillance	**12,28%**	**24,28%**	**29,82%**	**7,39%**	16,71%	24,19%
Unwanted content and/or behavior	**12,00%**	**24,84%**	**26,78%**	**6,83%**	16,62%	**24,84%**

(N=1.083)

Slightly less *respondents originating from Wallonia* than one would expect, **stop or avoid certain online activities** in order to secure their online experience, compared to *respondents from Flanders* (43,0% versus 52,5%, X^2(2)=11,69, N=1.036, p<.01). A majority of higher educated people, respectively 55,4% of *higher non-university/bachelor's* and 61,8% of *(post-)graduate/master's* degrees chooses to, among other things, stop or avoid activities online (X^2(7)=14,70, N=1.033, p<.05). *Brussels residents* tend to **change their settings** more often, we learn from 59,1% that indicated so (X^2(2)=8,46, N=1.036, p<.05). What is truly interesting, is that 64,6% of the youngest respondents, aging between *18 and 35 years old*, adjusts settings, while only 31,6% of the *elderly (65+)* does so in protecting themselves against cyber threats (X^2(4)=59,07, N=1.036, p<.001). Further, it seems that the better educated one is, the more he/she adjusts settings, with 63,6% of university degrees and 17,9% of the people without any degree doing so (X^2(7)=47,83, N=1.033, p<.001).

A majority (55,9%) of the self-employed/professionals **creates (a) back-up(s)**, therefore indicating the importance to them of safeguarding valuable information and preventing it from getting lost (X^2(10)=18,71, N=1.034, p<.05). Middle-aged people are more likely to **pay for protective software** than younger people are, with 48,6% of the 45-54 and 36,1% of the 18-34 years olds indicating that they take such protective measures (X^2(4)=12,47, N=1.036, p<.05). The reverse is true for **free software**, with 62,5% of the youngest and 49,0% of the middle-aged having it installed (X^2(4)=13,08, N=1.036, p<.05). People without diploma seldom have paid security software installed: only 15,4% of them does (X^2(7)=20,17, N=1.033, p<.01).

Within their age group, three times as many young people (aging 18-34) do not take protective measures against **scams**, compared with the number of elderly (aging 65+): 16,1% versus 5,1% (X^2(4)=17,38, N=1.036, p<.01). Almost half (47,0%) the people that do not take protective measures against scams, have completed a higher education, university or non-university (X^2(7)=24,53, N=1.033, p<.01). Of those that do not protect themselves against **hacking**, the majority is female (61,1%, X^2(1)=5,95, N=1.036, p<.05). A larger than expected number of university graduates (17,3%)

has no protection against hacking in place, at least not one of the prelisted measures $X^2(7)=14,39$, N=1.033, p<.05).

It seems that the older respondents in our sample feel the need to protect themselves against **governmental surveillance** more than young people do, with respectively 9,2% and 21,8% of both age groups having no protection in place ($X^2(4)=19,08$, N=1.036, p<.01). The same, but to a lesser degree, can be said about **corporate surveillance**: here 8,2% of the older versus 17,5% of the younger people are not protected by one of the prelisted safety measures ($X^2(4)=13,68$, N=1.036, p<.01). Higher educated people feel more confident about possible intrusions by government institutions and private companies: respectively 34,5% and 28,2% of them do not feel the need to protect themselves against these phenomena ($X^2(7)=33,74$, N=1.033, p<.001; $X^2(7)=24,01$, N=1.033, p<.01).

The youngest respondents seem to care less about witnessing **unwanted online content and/or behavior**: 21,1% of them do not take any protective measure against such encounters, while only 9,2% of the category between 55 to 64 years old and 9,7% of the 65+ years old refrain from security measures ($X^2(4)=17,87$, N=1.036, p<.01). As is the case with the above-mentioned threats, university graduates are most remarkable considering the lack of protection against unwanted content and/or behavior: not less than 34,5% see no danger and fails to take any security measure against the threat ($X^2(7)=39,60$, N=1.033, p<.001). Quite a few (35,3%) self-employed/professionals lack security measures, when it comes to unwanted content and/or behavior ($X^2(10)=41,27$, N=1.034, p<.001).

Next, we take a look at the total number of security measures people use to protect themselves from the various sorts of cybercrimes (see Figure 12). Most respondents (30%) use two security measures, followed by one measure and three measures (each 24%). Results show that one in ten people from Brussels (10,4%), have five out of six security measures in place, making them well-protected against various threats ($X^2(12)=27,05$, N=1.036, p<.01). Almost half the people (43,7%) that only take one security measure reside in Wallonia. Again, almost half of the people (46,3%) that take five measures are younger than 35, while only 9,3% of the group older than 64 years old do so ($X^2(24)=43,72$, N=1.036, p<.01). A one-way ANOVA analysis confirms that these two age categories differ significantly from each other (F (4, 1031) = 4,26, p<.01): 2,70 versus 2,30 (Δ = 0,40). People with a lower educational level take less security measures, as people who have *no diploma* or a *primary school diploma* add up to 29,3% of those that only have one measure in place within their age group ($X^2(12)=46,12$, N=1.033, p<.001). On the other hand, of those respondents who have a diploma in higher education, only 16,2% takes just one security measure, whereas 9,6% have five measures in place (versus 3,4% within secondary education and 1,3% within no/primary education). A one-way ANOVA shows that the three subgroups (no/primary education, secondary education, higher education) differ significantly from each other with respect to the amount of measures they take (F (2, 1030) = 16,40, p<.001). People who attended secondary education, take more protective measures than people with no/primary education (p<.05), whereas people with a higher education diploma take more measures than they who attended secondary education or have no/primary education (p<.001).

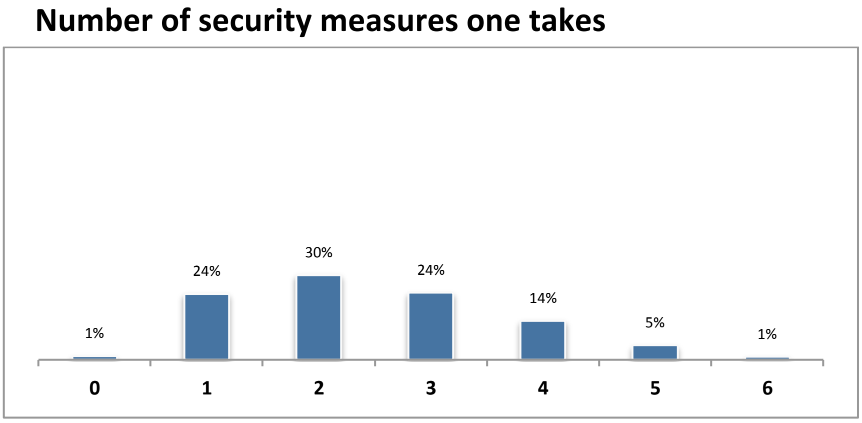


Figure 12: The number of security measures (with a maximum of six) one takes to protect him-/herself against cyber threats (N=1083)

In the next part, we look closer at the total number of threats people protect themselves against (see Figure 13). A large majority of 76% seeks protection against all six threats. In contrast of previous findings, young people (aged between 18-34 years old) protect themselves against significantly less threats than the elderly (aging 65+): 5,09 versus 5,62 (Δ = 0,53), F (4, 1031) = 5,24, p<.001. People with a higher education degree seem to outweigh people with a secondary education degree when it comes to protecting oneself and/or their family against multiple threats (F (2, 1030) = 9,38, p<.001). Strangely enough though, the group of higher educated does not differ significantly from the people that have attended no/primary education. **Combined with the findings above, one could state that younger and higher educated people seek protection with multiple security measures against various threats, but not against one threat in particular.**

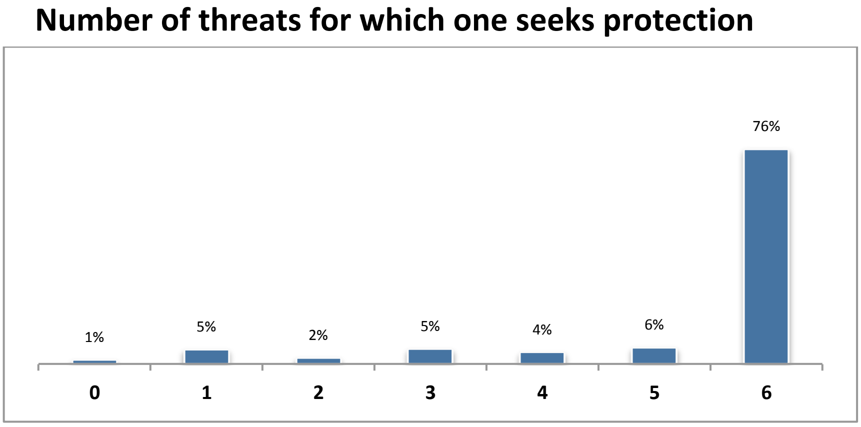


Figure 13: The number of threats (with a maximum of six) against which one protects him-/herself (N=1083)

When reducing the number of variables that represent the security measures one takes, a second factor analysis was performed (see Table 3). Following the first analysis, the sum variables, that add up to a total number of protective measures one takes against an equal number of threats, were used to include the number of threats in our analysis. As in the first factor analysis, another possibility for performing this analysis is with binary variables: did the respondent take the security measure, regardless of the number of threats against which he/she takes the protective measure? Here, both approaches yield slightly different results. For reasons of analogy, as well as to take the number of threats one protects him-/herself against into consideration, we base ourselves on the sum instead of the binary variables.

The variables can be reduced to three distinct categories of factors. A first factor, encompassing the reduction of the internet use and stopping or avoiding certain online activities, can be summarized as a general decrease in online activity (α=.17). Here, protection relies on inaction or constraints rather than taking action (the so-called maladaptive coping behavior). The second component represents both changing settings and creating a backup (α=.30). It rather deals with the terms and conditions of use and changing preconditions or functionalities of software, networks, hardware, accounts or websites. Creating a backup was once a safety measure that required deliberate action (e.g. copy pasting files to an external hard drive). Today, this implies more opting in or out a certain setting, which automatically creates a virtual copy. The third and last component represents more (pro-) active security measures (adaptive coping behavior). It concerns with having paid and/or free software installed that protects the user from various types of malware or intrusions. Here we notice how having free software installed has negative factor loadings on this third component, since it considers a substantively similar security measure, yet people seem to either pay for the software or they do not. For this reason, and because of the low internal consistencies of the first two factors, it was decided to proceed with all six variables (measures) separately.

Table 3: *Rotated factor loadings of security behavior sum variables*

	Loadings		
	Active measures	**Changing functionalities**	**Inactive measures**
Reduce internet use			**.67**
Stop or avoid certain activities		.33	**.70**
Change settings		**.74**	
Creating a backup		**.75**	
Install software (paying)	**.82**		
Install software (free)	**-.78**		-.30
Initial eigenvalue	1,38	1,27	1,09
Variance (%)	22,91	21,14	18,21
Rotated variance (%)	21,79	20,67	19,79

Rotated Component Matrix
Extraction method: PCA
Rotation method: Varimax with Kaiser normalization
Bartlett's Test of Sphericity: .00 sig.
Three components explain 62,25% of the variance (loss of 37,75%).
Factor loadings < .30 are not withhold.

The same can be done with the threats against which one protects him-/herself. Surprisingly, only one factor can be detected when performing the third factor analysis (see Table 4). This suggests that all six threats are seen as one phenomenon against which protection is needed. This finding calls in favour of using a collective noun like 'cybercrime' when talking about all threats associated with online activity. Indeed, when protection is in place, which is certainly the case for most of the people, a majority of the respondents (76,1% or more than three quarter of respondents) protects itself against all six prelisted threats (see Figure 12). This comprehensive protection consists of a variety of different security measures, as is suggested by Figure 11 (cfr. supra). Our respondents seem to introduce a couple of protective measures (mostly two) to safeguard their online activities, and neither rely on a singular solution, nor on the full range of protective measures (see Figure 13).

Table 4: *Factor loadings of threat security behavior sum variables*

	Loadings
	Cybercrime
Threat: viruses	**.70**
Threat: scams	**.83**
Threat: hacking	**.86**
Threat: governmental surveillance	**.85**
Threat: corporate surveillance	**.89**
Threat: unwanted content and/or behavior	**.82**
Initial eigenvalue	4,11
Variance (%)	68,53

Component Matrix
Extraction method: PCA
Bartlett's Test of Sphericity: .00 sig.
One component explains 68,53% of the variance (loss of 31,47%).

1.3 Conclusion

The Belgian internet user is quite active on the internet, though more at home than at work. This is especially the case for elderly people and people who reside in Wallonia. As for internet use at home, people with a higher education degree and/or minor children seem to make the least use of internet. As expected, younger people seem to make the most use of internet at home.

The Belgian internet user employs the internet to perform a range of different activities. These can be split into two broad categories, being traditional activities like news retrieval or e-mailing and more active social activities like using social media platforms, online gaming, etc. Especially the traditional activities are well integrated in the internet use of the Belgian user. As expected, younger respondents engage in online social activities a lot more than older people do.

When looking at how these activities are perceived in terms of their safety, the traditional activities are roughly seen as safer than the social activities. Purchasing and/or selling goods online (see Figure 10), downloading and being active on social media platforms are seen as the most unsafe activities. Overall, Belgians have little trust in the safety of the internet.

Almost all our respondents take security measures to protect themselves from cybercrimes. This takes the form of maladaptive coping behavior like avoiding or stopping activities but also more active adaptive coping behavior like the installation of (free) software. The Belgian internet user is least likely to reduce his time spent online in order to avoid victimization. Overall, people who live in Wallonia, elderly people, and people with a lower education level seem to take less security measures.

If we look at the total amount of threats people protect themselves against, a large majority seeks protection against all six predefined threats. Though, in contrast of what one would expect, young people protect themselves against less threats than elderly. Overall, higher educated people seem to protect themselves against more threats than those who are lower educated.

1.4 Profiles of the internet users

Throughout the remainder of this report, we describe the results comparing different profiles. This segmentation of the Belgian internet user is based on four factors pertaining to online activity and security:

1. **Frequency of internet use** – based on the average frequency of internet use at home and work during work days, and during the weekend;
2. **Variety of internet use** – based on the number of different devices on which traditional and social activities are practiced. The activities 'streaming' and 'purchase and/or sell goods' were excluded, for reasons mentioned above;
3. **Variety of security measures** – based on the number of security measures in place and the number of threats against which protection is sought. A distinction is made between maladaptive and adaptive coping behavior;
4. **Perceived safety of the internet –** based on the overall confidence in the safety of internet and the perceived safety of internet-related activities.

The cluster analysis resulted in four different clusters. These are prototypically labelled and discussed more in detail below.

A. Profile 1 - The conscious internet users (32,0% of the sample)

Frequency of internet use

Of the four different profiles, **the conscious internet users** make most use of the internet in their professional context: 39,3% of them is *more than one hour per day online at work* (χ^2 (15, N=1.083) = 44,42, p<.001). Especially compared to the **overly confident internet users (Profile 2)**, the conscious internet users make more use of internet during working hours (Kruskal-Wallis test: χ^2 (3, N=1083) = 31,87, p<.001). The same can be said about their internet use at home during weekends, with 40,2% of them being *online for more than three hours on an average weekend day* (χ^2 (15, N=1.083) = 32,08, p<.01). We have to say, however, that the contrast here is stronger with the **inexperienced users (Profile 3)** (Kruskal-Wallis test: χ^2 (3, N=1083) = 20,60, p<.001). Although 78,3% of the conscious internet users are *more than one hour per day online at home on an average work day,* this profile is not the most active profile when it comes to internet use at home during work days. Though, the differences between the different profiles are rather small. Only the **inexperienced users** are significantly less active at home during work days than the other profiles (Kruskal-Wallis test: χ^2 (3, N=1083) = 21,21, p<.001).

Variety of internet use

Besides *traditional activities*, the conscious users practice online *social activities* a lot. More than a fifth of them engage in *all five prelisted social activities*, whereas only 8,4% do *no social activity at all* (χ^2 (15, N=1.083) = 54,47, p<.001). Certainly compared to the **inexperienced internet users**, the conscious users indeed engage more in traditional and social online activities (F (3, 1082) = 12,16, p<.001 and F (3, 1082) = 14,89, p<.001). Even more remarkable, when looking at the total number of unique activities: almost half (46,5%) of the number of conscious internet users has practiced *nine or more (out of eleven) different online activities* in the last month (χ^2 (33, N=1.083) = 92,05, p<.001). Again, compared to the **inexperienced** (*M* = 6,67, *SD* = 2,53), but also the **overly confident users** (*M* =

6,97, *SD* = 2,30), the conscious internet users (*M* = 8,04, *SD* = 2,30) involve significantly more in online activities (F (3, 1082) = 21,24, p<.001). All this gives makes us conclude that these users are by far the most IT literate, in a technical sense.

Not less than 39,9% of the conscious internet users have *four or more devices* at their disposal, remarkably more than any other profile (χ^2 (15, N=1.083) = 62,26, p<.001). In comparison, the conscious internet users have significantly more devices (*M* = 3,06, *SD* = 1,23) than the **overly confident** (*M* = 2,29, *SD* = 1,20) and the **inexperienced internet users** (*M* = 2,60, *SD* = 1,22, F (3, 1082) = 15,42, p<.001).

Variety of security measures

The conscious internet users are more concerned with adjusting settings and securing their files through back-ups. Almost nine out of ten (89,3%) users within this group *change certain settings* in order to make the time spent online more safe (χ^2 (3, N=1.083) = 410,83, p<.001). This suggests that the conscious users understand the online environment quite well, since they control the functionalities of their software (e.g. browser) or the web pages that they visit (e.g. social media platforms). These users will leave nothing to chance: they add up to over half (50,7%) the users that *make (a) back-up(s)* (χ^2 (3, N=1.083) = 88,64, p<.001). This strongly suggests that data-protection is very important to them, whether this means protecting important files from getting corrupted, or their privacy and thus personal data by adjusting settings. The conscious users will *avoid certain online activities* though, when risks are perceived as too high. A clear majority (66,2%) within this group indicated they took such protective measure (χ^2 (3, N=1.083) = 149,19, p<.001). All together, the conscious internet users rely more on adaptive protective measures (73,8% of the total amount of measures), this in contrast to the **inexperienced internet users** (45,7%). **The overly confident internet users** (95,3%) and, to a lesser extent **the resolved internet users (Profile 4)** (88%), barely engage in maladaptive coping behavior.

As expected, the conscious internet users have by far the most security measures in place, compared with other profiles (*M* = 3,22, *SD* = 1,17, F (3, 1082) = 107,40, p<.001). Respectively 58,8%, 69,6% and 90,9% of those that take *four, five and six security measures*, are conscious internet users (χ^2 (18, N=1.083) = 362,62, p<.001). Like all other profiles – the **inexperienced users** to a significant lesser extent however (cfr. infra) – the conscious users seek protection against all six prelisted threats. A large majority (85,5%) of these users do so against *all six threats*. Only 0,9% of users with this profile protect themself against *fewer than four threats*. The only profile that differs significantly from the conscious users (*M* = 5,80, *SD* = 0,54), concerning the number of threats against one seeks protection, is that one of the **inexperienced users (***M* = 4,31, *SD* = 2,10, F (3, 1082) = 104,01, p<.001).

Perceived safety of internet-related activities

Most (83,8%) of the conscious internet users know what *online gaming* is, or how to assess its safety (χ^2 (15, N=1.083) = 36,21, p<.01). They also form the majority (42,3%) of those that believe it to be *not safe at all*. Significantly less conscious users do not know what or how safe *e-commerce, social media, downloading, streaming, chatting* and *phone calls over the internet* are, compared to other profiles. These percentages range from 4,6% for e-commerce (χ^2 (15, N=1.083) = 36,17, p<.01) to 14,5% for VoIP (Voice over IP) services (χ^2 (15, N=1.083) = 30,02, p<.05). This is a further indication that they certainly do not lack experience with the internet. Four out of ten (41,1%) users that see

VoIP (Voice over IP) services as safe, a finding that fits this profile (χ² (15, N=1.083) = 30,02, p<.05). When we take a look to the average perceived safety of the combined internet activities (*M* = 2,93, *SD* = 0,70, 1 indicating not safe at all, 5 indicating very safe), we see no significant differences in comparison to the other profiles.

Interestingly, almost half the number of people (46,1%) that reside in *Brussels* fit this profile (χ² (6, N=1.036) = 17,28, p<.01). The conscious internet users are significantly younger than other profiles, with the biggest difference of over six years with the **overly confident internet users** (*M* = 43,94, *SD* = 15,04 versus *M* = 50,23, *SD* = 15,01, F (3, 1035) = 8,61, p<.001). A majority (34,7%) of the conscious internet users is younger than 35, or, stated otherwise, 40,4% of the people within *age category 18-34* belong to the conscious internet user profile (χ² (12, N=1.036) = 34,62, p<.01). These users seem higher educated in comparison to the other profiles, given the fact that 40,5% has a *higher non-university or university degree*, as opposed to the **overly confident internet users** (27%), the **resolved internet users** (22,1%) and to a lesser extent the **inexperienced internet users** (32,6%) (χ² (21, N=1.033) = 61,97, p<.001).

The conscious internet users are young, highly-educated citizens who makes daily use of the internet. As well in work settings, as at home, they regularly spend between one and three hours online, or even more. They use this time for a variety of activities, ranging from e-mailing and information retrieval to chatting and social media, and use multiple devices to do so. Although the conscious internet users are highly IT literate and have a relative high trust in IT, they take no risks and take multiple security measures to protect themself against various kinds of threats.

B. Profile 2 - The overly confident internet users (13,5% of the sample)

Frequency of internet use

The **overly confident internet users** seldom go on the internet for work, seeing that a majority (62,3%) of them *never accesses the internet at work* (χ² (15, N=1.083) = 44,42, p<.001). This is an interesting contrast with the respondents of the profile the **inexperienced users (Profile 3)**, who are instead not that active online in their spare time (cfr. infra).

Variety of internet use

Most overly confident users only have *one device* at their disposal to connect to the internet (32,2%, χ² (15, N=1.083) = 62,26, p<.001). Perhaps they do not feel the need to possess multiple devices, when they can do the majority of their activities on one device. In this respect, they form the counterpart of the **conscious internet users**.

The variety of activities they engage in, forms another interesting divide between both profiles: a fifth of the overly confident users (20,5%) engage in *seven different activities (out of eleven)*, both traditional and social activities, making them take part in a greater variety of activities than the **inexperienced users** (χ² (33, N=1.083) = 92,05, p<.001). They do seem to lack experience with *e-commerce, downloading* and *streaming*, seeing that this profile represents respectively 23,2%, 20,8% and 19,9% of those that do not know what or how safe these activities are (χ² (15, N=1.083) = 36,17, p<.01; χ^2 (15, N=1.083) = 43,77, p<.001; χ^2 (15, N=1.083) = 41,67, p<.001). This finding makes us assume that the respondents belonging to this profile have quite some confidence in the safety of internet-related activities.

Variety of security measures

The security measures that the overly confident users take, seem to be the product of a personal cost-benefit analysis. In a sense, they are economical rational users, who will certainly not miss out on opportunities that the internet has to offer, and do not reduce their internet use or stop/avoid certain internet-related activities in order to protect themselves against various threats (maladaptive coping behavior, cfr. supra). Only 5,5% of these users do *reduce the time spent online* (χ^2 (3, N=1.083) = 64,43, p<.001). In this respect, they form the counterpart of the average **inexperienced users** (cfr. infra). Likewise, they add up to a mere 3,5% of those who *stop or avoid internet activities* (χ^2 (3, N=1.083) = 149,19, p<.001). The confident users will not waste time figuring out how to deal in a sensible way with software or web pages or by creating a back-up of their important data. Only 2,8% of the respondents who *adjust settings* to secure their connection (χ^2 (3, N=1.083) = 410,83, p<.001), and 6,2% that *create (a) back-up(s)* (χ^2 (3, N=1.083) = 88,64, p<.001), fall under this group. These users will certainly not pay for protective software, when it is available for free. These users form by far the minority (0,4%) among those who decided *to pay for such protection* (χ^2 (3, N=1.083) = 376,65, p<.001). It makes more sense to them to just download and install protective software without charge, since according to them it serves mainly the same purpose to a lower cost. All of them (100,0%) have *free software installed* on their device(s), that offers protection online (χ^2 (3, N=1.083) = 297,00, p<.001).

An large majority (65,8%) of these users have only *one security measure* in place (χ^2 (18, N=1.083) = 362,62, p<.001). This suggests that the overly confident users are certain that this free software will offer protection against all sorts of threats. What certainly feeds this assumption, is the fact that almost all (97,9%) overly confident users believe they are protecting themselves against *all six predefined threats* (χ^2 (18, N=1.083) = 281,42, p<.001).

Perceived safety of internet-related activities

Compared to other users, and certainly the **inexperienced users** (F (3, 962) = 3,13, p<.05), the overly confident internet users believe *social media* to be quite safe. They make up only 9,4% of those stating that social media are not safe (χ^2 (15, N=1.083) = 36,00, p<.01). The same can be said about *online gaming*: almost a third (28,2%) of those that indicated online gaming to be very safe, belong to this group (χ^2 (15, N=1.083) = 36,21, p<.01). Although this difference is not significant, the overly confident internet users also account for the highest average perceived safety of the combined internet activities (*M* = 3,02, *SD* = 0,67). Also, these users score the highest on the internet-confidence scale (F (3, 1082) = 3,08, p<.05). Although the difference in mean scores is rather small, the **inexperienced internet users** are significantly less confident about the safety of the internet: 2,88 versus 2,68 (Δ = 0,20). All this feeds the assumption that the overly confident internet users have quite some confidence in the safety of internet-related activities.

Compared to the conscious internet users, the overly confident internet users are the oldest of our user profiles (*M* = 50,23, *SD* = 15,01 versus *M* = 43,94, *SD* = 15,04, F (3, 1035) = 8,61, p<.001). More than a quarter (25,6%) of the respondents *without diploma* fit this profile, compared to only 4,5% of the ones with a *university degree* (χ^2 (21, N=1.033) = 61,97, p<.001). Given the smaller portion of our sample that identifies with this profile (13,5%), the deviation from the expected number of people without diploma is greater than is the case with the inexperienced internet user profile (vide infra). This suggests that the overly confident internet users are less educated than other users.

The overly confident internet users are older, rather low educated individuals who make use of the internet on a daily basis. Although they use internet mainly at home and not so much in a work setting, the overly confident internet users regularly spend between one and three hours online, or even more. They use this time for a variety of activities, traditional as well as social activities, but have less experience with activities like e-commerce, downloading and streaming. Furthermore they mostly use just a single device to engage in these activities. The overly confident internet users have great confidence in the safety of the internet and believe that taking one or two security measure is enough to protect themselves against most threats. If they have to choose a security measure they would rather install free software than pay for it, reduce their time spent online, or stop certain activities.

C. Profile 3 - The inexperienced internet users (35,5% of the sample)

Frequency of internet use

The **inexperienced internet users** are remarkably less *online when at home during work days* or *at weekends*. They represent 65,0% of those respondents that go online *less than weekly when at home during work days* (χ^2 (15, N=1.083) = 31,66, p<.01), and 66,7% of those that *never go online during weekends* (χ^2 (15, N=1.083) = 32,08, p<.01).

Variety of internet use

The inexperienced users constitute the majority (50,7%) of those respondents who do not engage in any online *social activity* (χ^2 (15, N=1.083) = 54,47, p<.001). With 49,4%, the inexperienced users form the centre point of those who engage in *four unique online activities* (χ^2 (33, N=1.083) = 92,05, p<.001). All of these findings make us conclude that the respondents belonging to this profile lack experience with the internet and could be ill-informed about threats one might encounter on the internet and how to tackle them. As their profile name suggests, these inexperienced users are by far the least IT literate. Somehow surprisingly though, they do use multiple devices (*M* = 2,6, *SD* = 1,22), 51,5% uses more than two.

Variety of security measures

The inexperienced internet users do not secure their online experience all too much. The only security measures they seem to take is reducing the time spent online and, to a lesser extent, stopping or avoiding certain activities (maladaptive coping behavior). This profile represents a majority (55,1%) of those respondents who *reduce their internet use*, which indicates they can also be considered deterred internet users (χ^2 (3, N=1.083) = 64,43, p<.001). Their portion within the group of respondents who *stop/avoid certain internet-related activities* is somewhat smaller, but can still be considered high: 41,2% (χ^2 (3, N=1.083) = 149,19, p<.001). Three quarter (75,5%) of the inexperienced users do not *change settings*, making them the largest subgroup (50,2%) within the respondents who indicated they do not take such protective measures (χ^2 (3, N=1.083) = 410,83, p<.001). Nor do they *make (a) back-up(s)*: again three quarter (77,6%) do not have the knowledge or feel the need to do so (χ^2 (3, N=1.083) = 88,64, p<.001). A majority (67,7%) of these users are not inclined to *pay for protective software* (χ^2 (3, N=1.083) = 375,65, p<.001). All (100,0%) of the internet users who have *not one security measure* in place, and thus that can be considered as not well protected at all, are inexperienced internet users (χ^2 (18, N=1.083) = 362,62, p<.001). Almost four out of then (39,6%) of these inexperienced users still have *two security measures* in place.

Likewise, all (100,0%) of the users that take protection against *not one threat*, and of those that only protect themselves against *one threat*, fit the inexperienced users profile (χ^2 (18, N=1.083) = 281,42, p<.001). 54,9% of the inexperienced users protect themselves against *all six threats*, by far the smallest percentage when compared with other profiles. The fact that most users (76,1%, see Figure 12) protect themselves against all six predefined threats further emphasizes the inexperienced users' low level of protection.

Perceived safety of internet-related activities

Although this difference is not significant, the inexperienced internets user account for the lowest average perceived safety of the combined internet activities (*M* = 2,87, *SD* = 0,68). Also remarkable is that, compared to the **resolved internet users** (vide infra), only few inexperienced users believe *online banking* is very safe: respectively 21,7% versus 9,9% do (χ^2 (15, N=1.083) = 37,96, p<.01; F (3, 1062) = 2,76, p<.05).

Slightly more *women* (39,0%) than *men* (31,3%) fit this profile (χ^2 (3, N=1.036) = 8,62, p<.05). Over half the people *without any diploma* (51,3%) are inexperienced users (χ^2 (21, N=1.033) = 61,97, p<.001). However, as explained above, the deviation from the expected count is smaller for these users, than is the case with the **overly confident users** (due to their larger group size). Either way, one could say the inexperienced internet users have a rather low educational level, though not as low as the **resolved internet users** and, even more, the **overly confident internet users**. The average age of this profile group (M = 48,7, SD = 15,85) does not differ significantly from the other profiles.

The inexperienced internet users are older, less educated individuals who do not make much use of the internet. If they use internet, this is mostly in a work setting and not at home. The inexperienced users only engage in a few traditional activities like e-mailing or information retrieval, but have very little experience with social activities. Notwithstanding this low activity, they possesses multiple devices to access internet. The inexperienced internet users are not IT literate, have a rather low confidence in the safety of internet and take little security measures. When they do so, they would rather reduce their time spent online or stop certain activities, than take up security measures that ask a certain amount of IT knowledge. Consequently the inexperienced users are poorly protected against most security threats.

D. Profile 4 - The resolved internet users (19,1% of the sample)

Frequency of internet use

The **resolved internet users** are quite active on the internet, considering that 81,7% of them is more than one hour *online when at home during work days* and 79,2% of them during weekends. When it comes to internet use at work, the resolved internet users show a similar profile to that of the **inexperienced internet users (Profile 3)**. Indeed, they are quite active internet users during work days (30%), more than the **overly confident internet user (Profile 2)** (19,2%), but less than the **conscious internet user (Profile 1)** (39,3%).

Variety of internet use

The resolved internet users have significantly more *devices at their disposal* than the **overly confident internet users** (*M* = 2,77, *SD* = 1,35 versus *M* = 2,29, *SD* = 1,20, F (3, 1082) = 15,42, p<.001). They engage more in *traditional* and *social activities* than the **inexperienced internet users** do (F (3, 1082) = 12,16, p<.001; F (3, 1082) = 14,89, p<.001). For social activities, this contrast is not as explicit as is the case with the **conscious internet users**; for traditional activities, however, the situation is more clear. The fact that the resolved internet users engage in a significantly larger number of unique online activities, serves as an important point that allows to differentiate them from the **inexperience internet users** (F (3, 1082) = 21,24, p<.001).

Variety of security measures

The resolved internet users seem to be well aware of internet threats, since they rely on paid software that offers protection while being connected to the internet. Almost all (97,6%) the resolved internet users have *paid software* installed (χ^2 (3, N=1.083) = 376,65, p<.001). Reversely, it should be no surprise that only one out of ten resolved users have *free software* installed (χ^2 (3, N=1.083) = 297,00, p<.001). Presumably, internet security is a significant problem to them, since they are willing to pay for software that safeguards them on the world wide web. Maybe the respondents belonging to this user profile are also overly confident that software will grant protection against all sorts of threats one might encounter online, since it is the only protection they seem to take. Reducing their internet use is not an option: after the **overly confident users**, the resolved internet users are second least likely to spent *less time online* in order to avoid threats (10,1%, χ^2 (3, N=1.083) = 64,43, p<.001). Nor are they inclined to *stop or avoid certain online activities*: 67,1% indicated they do not do so (χ^2 (3, N=1.083) = 149,19, p<.001).

Just as the **overly confident internet users** (cfr. supra), but to a lesser extent, the resolved internet users rely mostly on one security measure. A majority (36,2%) of the people within this profile indicated they only have *one security measure* in place (χ^2 (18, N=1.083) = 362,62, p<.001). However, the resolved internet users are less confident that this will provide protection against *all six predefined threats*. Unlike the **overly confident internet users**, 15,9% believes to have taken protective measures against *fewer than six threats* (χ^2 (18, N=1.083) = 281,42, p<.001).

Perceived safety of internet-related activities

Only 4,8% of the resolved internet users believe *online banking* to be not safe at all, suggesting they have more confidence in online monetary transactions in comparison to other profiles do (χ^2 (15, N=1.083) = 37,96, p<.01). Likewise, they add up to a majority (39,3%) of those who perceive *e-commerce* to be very safe (χ^2 (15, N=1.083) = 36,17,p<.01) and almost half (46,2%) of those who consider *downloading* to be very safe (χ^2 (15, N=1.083) = 43,77, p<.001). It seems that having paid protective software in place gives them the confidence to engage in activities that are generally seen as quite unsafe (see Figure 10).

Men form the majority (57,0%) within this profile (χ^2 (3, N=1.036) = 8,62, p<.05). A remarkable observation too, certainly in comparison to other profiles, is that more than a quarter (26,5%) of respondents *older than 64* fit well within this profile (χ^2 (12, N=1.036) = 34,62, p<.01). These users are indeed significantly older than the **conscious internet users** (*M* = 49,12, *SD* = 16,33 versus *M* = 43,94, *SD* = 15,04, F (3, 1035) = 8,61, p<.001). Only 22,1% of the resolved internet users have a higher education degree. And although only 3% of the respondents within this profile has no/primary education, 74,9% does only have a secondary education degree. All this suggests the resolved internet users have a rather low education level.

The resolved internet users are older, rather low educated individuals who quite often make use of the internet, both at home and in a work setting. The respondents belonging to this profile engage in multiple online activities, both traditional and social activities, and use multiple devices to do so. They take internet security quite seriously, and do not hesitate to pay for protective software. Although they realize this is not enough to protect themselves against all kinds of threats, they mostly stay with this one measure. Overall this gives them the confidence to engage in online activities that are considered unsafe by other people.

1.5 Conclusion

The Belgian internet user can be clustered into four different internet user profiles, based on four factors: frequency of internet use, variety of internet use, variety of security measures and perceived safety of the internet. These four profiles are the conscious internet users (Profile 1) (32%), the overly confident internet users (Profile 2) (13,5%), the inexperienced internet users (Profile 3) (35,5%) and the resolved internet users (Profile 4) (19,1%). Based on the different variables that have been used to construct this typology, we managed to distinguish between these profiles. As such, it became possible to identify relevant variability in the data at hand.

2 Cybercrime victimization

In this section we describe each type of cybercrime separately, to allow for a better insight into cybercrime victimization in Belgium. Therefore we treat different topics like their occurrence (including, when present, significant differences between socio-demographic variables and our four profiles), various crime-specific topics, their perceived severity, and how/if they are reported. In a last paragraph we describe the financial impact of the different kinds of cybercrime.

These statistics are exclusively descriptive and explorative of nature. Source of this data were open question we have included for each cybercrime category, by which we asked the respondents to briefly describe what exactly happened the last time he/she encountered such a crime. This question contributes to the uniqueness of the current study, allowing for a better interpretation of the data and a more in-depth, qualitative analysis of what exactly happened.

Cybercrime victimization

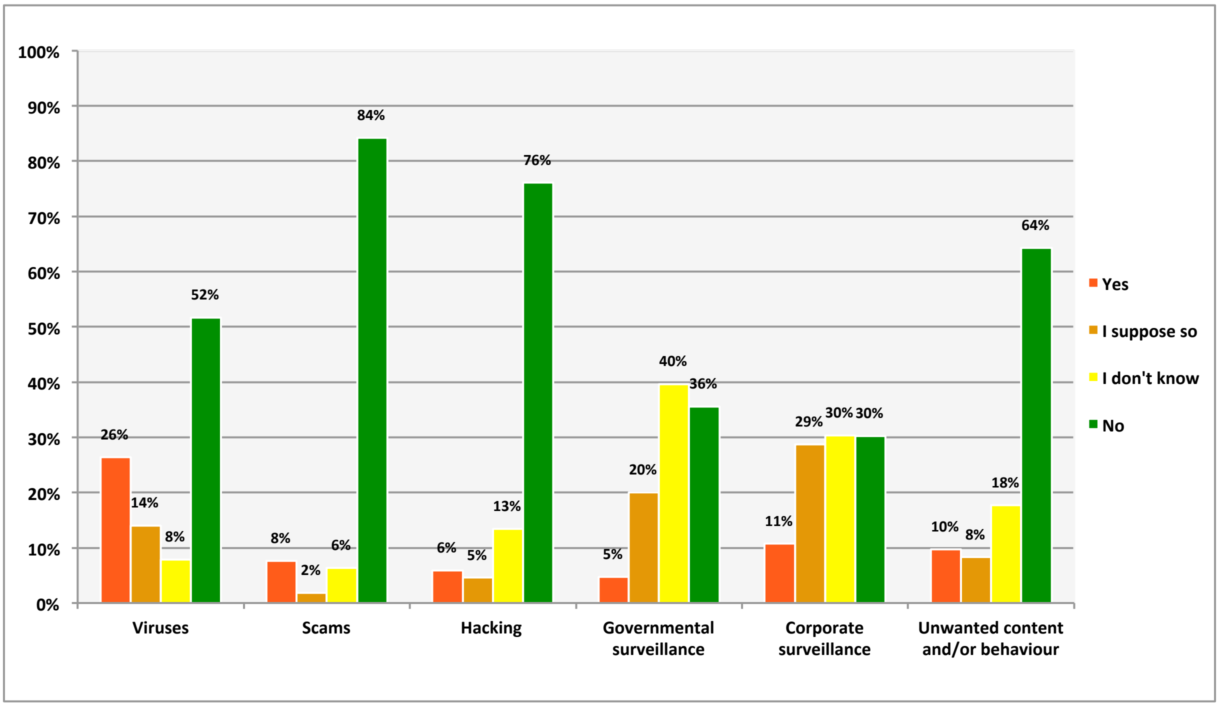


Figure 14: cybercrime victimization in the past year: 'Yes, myself', 'Yes, someone else in my family' and 'Yes, both me and someone else in my family' combined, but separated from 'I suppose so' (N ranges from 1.110 to 1.112)

Figure 14 and Figure 15 differ because in Figure 15 we have taken the answer categories 'Yes' and 'I suppose so' from Figure 14 together in one category 'Supposedly yes'. This allows for a more nuanced perspective on the victimization of cybercrime in the past year.

Cybercrime victimization (combined)

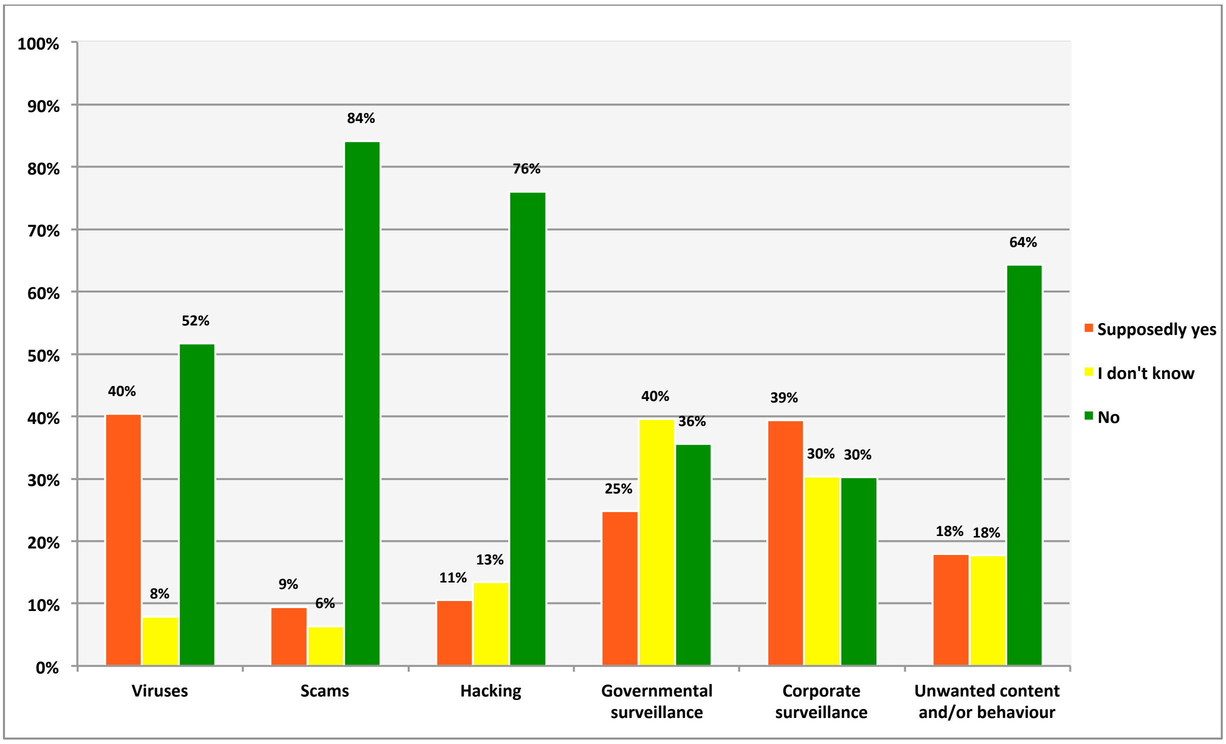


Figure 15: cybercrime victimization in the past year: 'Yes, myself', 'Yes, someone else in my family', 'Yes, both me and someone else in my family and 'I suppose so' combined in 'Supposedly yes' (N ranges from 1.110 to 1.112)

Based on Figure 14 and Figure 15 we can conclude that our respondents have been most often victim of the cybercrime type 'viruses'. 'Corporate surveillance' comes on the second place. The respondents have been least often victim of the cybercrime types 'scams', 'hacking' and 'unwanted content and/or behavior'. What is interesting is that for two categories, 'governmental surveillance' and 'corporate surveillance', the percentage of the answer category 'I don't know' is higher than for the other cybercrime types. It is also for these two categories that the difference between Figure 14 and Figure 15 is most interesting.

2.1 Viruses

Occurrence

Not surprisingly, viruses like malware or botnets remain the biggest threat in terms of occurrence and made the most victims during the last year (see Figures 14 and 15). More than a quarter (26,4%) of the general population is convinced of the fact that they themselves and/or someone else in their family became victim of at least one virus during the past 12 months (see Figure 14). This number rises to more than 4 out of then (40,4%) people when also taking into account those people that are not too sure about what happened, but suppose that they themselves and/or somebody in their family became a victim of viruses (14,0%, see Figure 15). Of those respondents that are certain about this, 55,6% (36,3% within the 'supposedly yes' group) became a victim themselves, 20,1% (13,1%) indicated that someone else in their family became a victim, and 24,2% (15,8%) answered that both they themselves and someone else in their family became a victim.

Table 5: *Breakdown by residence for virus victimization*

	Flanders	Wallonia	Brussels	Victimization total
Virus victimization - no				
- Percentage within 'no'	57,0%	32,1%	10,9%	100,0%
- Percentage within 'residence'	78,9%	68,3%	73,0%	74,5%
Virus victimization - yes				
- Percentage within 'yes'	**44,7%**	**43,6%**	11,7%	100,0%
- Percentage within 'residence'	**21,1%**	**31,7%**	27,0%	25,5%
Residence total	53,9%	35,0%	11,1%	100,0%
	100,0%	100,0%	100,0%	100,0%

(N=1.036, p = .002)

Compared to the other regions, more respondents residing in *Wallonia* are sure about having encountered a virus (see Table 5). Almost a third (31,7%) of them became a victim him-/herself or knows someone in their family who did, compared to 21,1% of the respondents residing in *Flanders* and 27,0% of the respondents residing in *Brussels* (χ^2 (2, N=1.036) = 13,00, p<.01). This divide also emerges when taking into account those that suppose such a crime to have happened: 45,5% of the respondents residing in Wallonia versus 35,3% of the respondents residing in *Flanders* and 39,1% of the respondents residing in *Brussels* at least suspect to have been victimized (χ^2 (2, N=1.036) = 9,50, p<.01). People who achieved an *upper secondary technical or art degree* as their highest education were more victimized in the last year than other educational levels: 34,3% indicated so (χ^2 (7, N=1.033) = 16,27, p<.05). Compared to other professional statuses, the respondents that are *incapacitated for work or on a long-term sick leave* suspect more to have become a victim of (a) virus(es) in the past year. More than half the number of these respondents (53,8%) indicated they do so (χ^2 (10, N=1.034) = 21,17, p<.05).

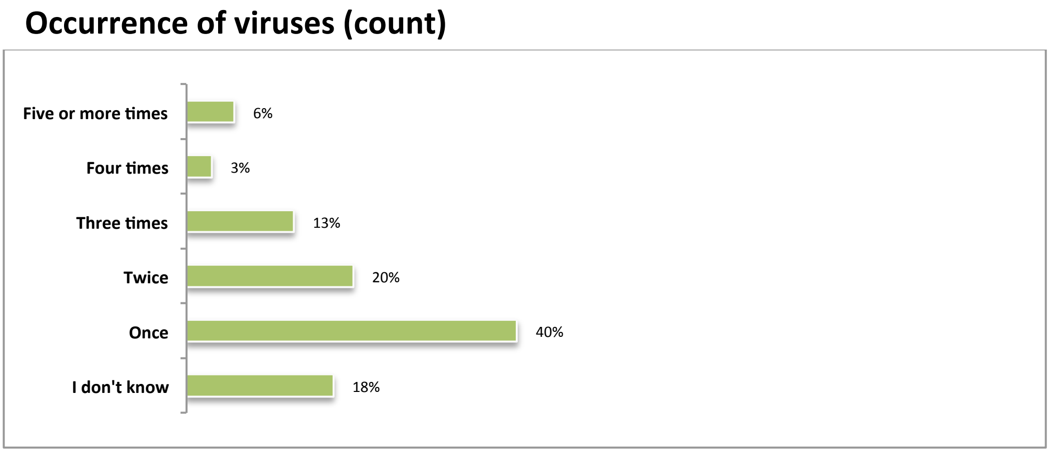


Figure 16: Number of times one became a victim of (a) virus(es) during the past year (N=292)

A vast majority of the 292 households that became victim of viruses in the past year encountered just one virus (40,1%, see Figure 16). Quite a large number of people (17,8%) do not know exactly how many viruses they became victim of, endorsing the fact that there appears some fuzziness around the phenomenon. 17 people (5,8%) experienced five or more viruses during the past year. Combined, these results suggest that viruses are a threat to which people are commonly exposed, certainly compared to other threats (see Figures 14 and 15).

Crime specific information

When we look at what exactly was damaged or got infected, we find that software malfunctions are most common (51,9% indicated 'yes'), followed by hardware (24,7%), files (18,8%) and, again, not knowing where the damage occurred (15,0%, see Figure 17). When a device failed to work properly, crashed or froze, it was mostly labelled as damaged hardware by the respondent. In further analysing the incident descriptions, we assume that quite a few people interpreted damaged or infected software as the virus itself. Reason for this assumption is that some respondents indicated that the virus formed no threat and merely was an attempt to cause harm, when apparently having experienced damaged software. However, these people cannot be isolated for further analysis, since the motivations for checking off a certain damage category are unclear.

Likewise, we can only suspect that sometimes (1) damaged or infected networks are misinterpreted as problems connecting to the internet or that occur while browsing the internet, instead of problems with the LAN or intranet, and (2) pop-up windows, website redirects, online advertisement, or even a homepage that has changed, are falsely considered to be damaged or infected websites, while in fact this damage category aims to measure damaged or infected websites, managed by the respondent him-/herself. Moreover, it is likely to have happened that someone checked off the 'I don't know' damage category, when really meaning to say that no damage had occurred. The absence of a 'no damage' category is likely to be the cause for this response bias. However, the omission of this answer option is arguable, since only victims of viruses were intended to see this question.

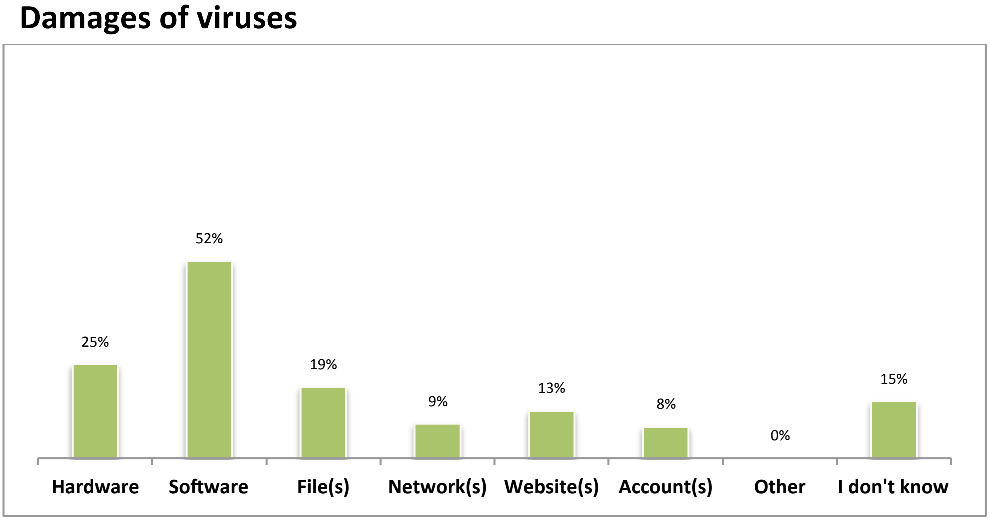


Figure 17: What exactly was damaged or got infected the last time you were victim of (a) virus(es)? (N=287)

Of the people that indicated how they got the virus, a large majority (48,5%) stated that they became a victim of one or multiple viruses while or after downloading (see Figure 18). This should be no surprise, given the proliferation of malicious software when illegally downloading content. These are followed by the ones that got (a) virus(es) through e-mail (27,3%).

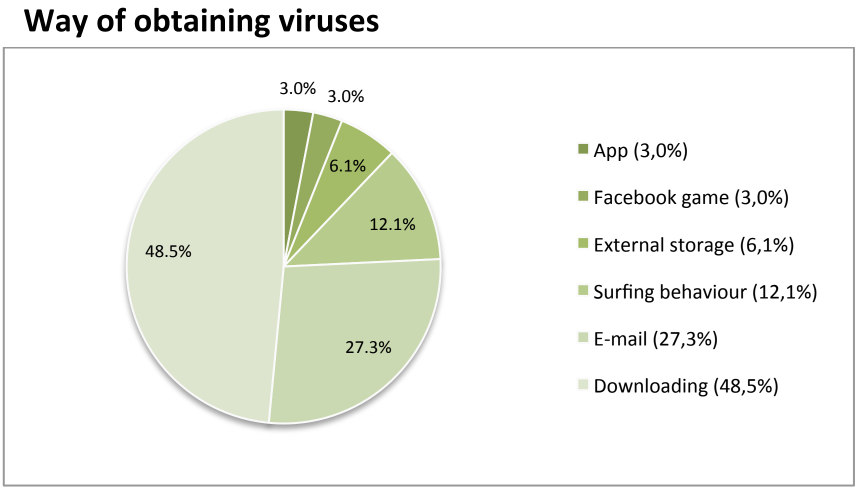


Figure 18: Through what medium was/were the virus(es) obtained?
(classifications distilled from descriptive answers, N=33)

Of the people that gave classifiable information considering what effect the virus had, other than the prelisted damage categories, a majority indicated that unsolicited content appeared (34,9%, see Figure 19). Most often these were commercial advertisements, pop-up windows or website redirects, not uncommon for sexual products or services. Almost a quarter (22,2%) of this subgroup of respondents deals with a slowing down of their device, and thus a considerable loss of time, due to the virus(es). Quite a few people (32 or 11,2% of the victims of viruses) state that they managed to overcome the virus, with or without having to recourse to external technical expertise.

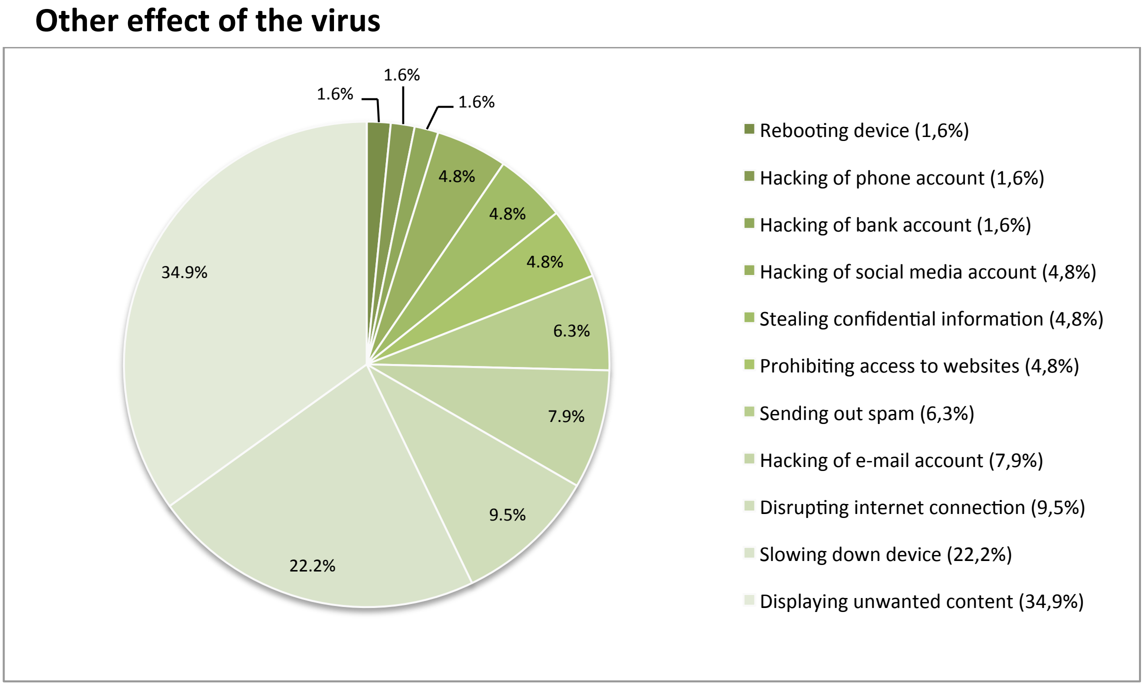


Figure 19: What other damaging effect did the virus have?
(classifications distilled from descriptive answers, N=63)

From the information that was given with regard to what kind of virus one became victim of, we found that 36,8% experienced Trojan horse malware, followed by police virus ransomware (31,6%, see Figure 20). The latter came as quite a surprise and can be understood as either malware that blocks the device, a web page redirect or a received mail, each time displaying a message (seemingly from the federal police) stating that illegal activity was detected and the victim needed to pay a fine (in order to allow further access/activity in case of a blocked device).

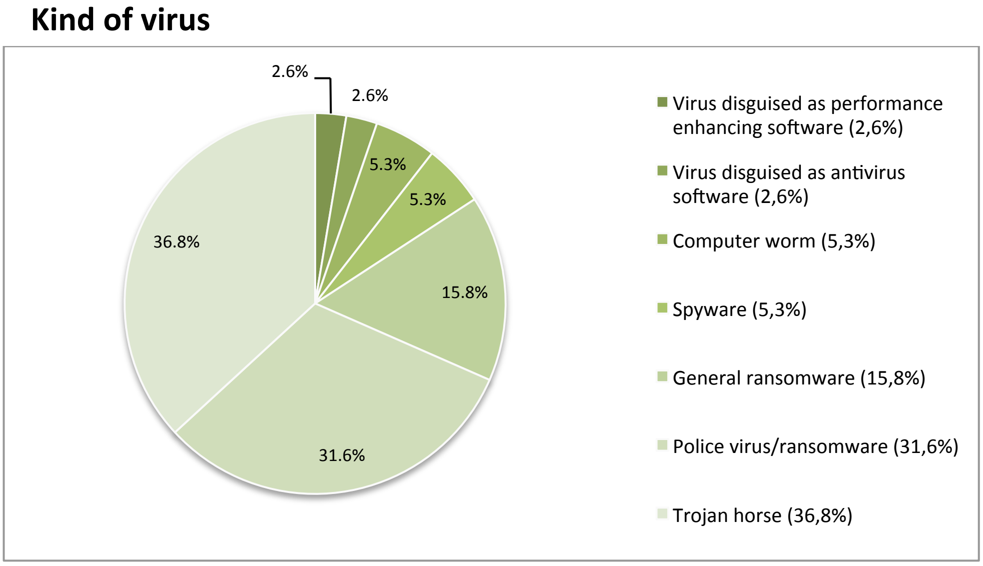


Figure 20: What kind of virus(es) did the respondent or their relative(s) last became victim of?
(classifications distilled from descriptive answers, N=38)

Perceived severity

All the cybercrime types that were questioned in terms of their severity are perceived as quite serious (overall *M* = 4,27). Perhaps unsurprisingly, our sample perceives **government surveillance** as the least serious internet crime (*M* = 3,93, *SD* = 0,93). **Hacking** and **scams** are seen as the most severe phenomena (respectively *M* = 4,59, *SD* = 0,66, and *M* = 4,56, *SD* = 0,70), followed by **viruses** (*M* = 4,36, *SD* = 0,69), **unwanted content and/or behavior** (*M* = 4,29, *SD* = 0,90) and **corporate surveillance** (*M* = 4,23, *SD* = 0,86).

The respondents belonging to Profile 2 – The **overly confident internet users** differ significantly from all of the other profiles, concerning the perceived seriousness of viruses (*M* = 4,16, *SD* = 0,80, F (3, 1082) = 4,70, p<.01). They think viruses are less serious, especially compared to the **conscious internet users** (Δ 0,24, p<.01).

Reporting

Only 15,4% (almost one in six) of the victims reported the incident, confirming the remark made by CERT.be that only a minority of cybercrime incidents are reported (see Figure 21). When an incident is reported, it is more often reported with the user's internet provider (8,4%) than with law enforcement institutions (4,2%). Of the twelve people (4,2%) that reported the incident with another body than those prelisted, five (42,2%) reported the infection with a repair service or the in-store customer support service, three (25,0%) with Microsoft (probably by means of an automatically generated problem report), and one (8,3%) each with the company behind the social network site (Facebook), their e-mail provider, financial institution, and employer. No significant differences between the four user profiles were found for any of the cybercrime types.

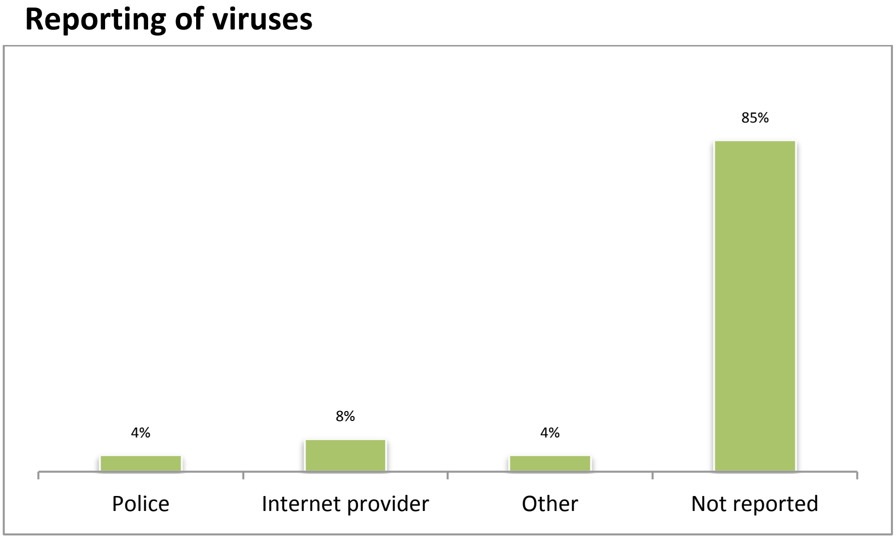


Figure 21: With which body was the last incident reported? (N=286)

2.2 Scams

Occurrence

More than one out of fifteen people (7,6%) encountered attempted or succeeded scams or have knowledge about scam victimization in their family during the last year (see Figure 14). Almost one out of ten people (9,4%) at least suspect that they themselves and/or someone in their family became victim of this type of cybercrime (see Figure 15). Online scams thus pose a significant threat when thinking about the financial losses that often result from this form of cybercrime. Of the victims, 44,7% (36,2% within the 'supposedly yes' group) is certain that they themselves became a victim, 27,1% (21,9%) believe that someone else in their family became a victim, and 28,2% (22,9%) that both they themselves and someone else in their family became a victim.

In line with the finding about viruses, people that reside in *Wallonia* seem to be more susceptible for online scams, in comparison to respondents residing in the other regions. Not less than half the number of people (48,1%) that are certain about having encountered a scam, reside in *Wallonia* (see Table 6, χ^2 (2, N=1.036) = 10,02, p<.01). A similar finding is being witnessed when looking at people that at least have a suspicion about being scammed: almost double the number of respondents residing in *Wallonia* (12,9%) indicated they came in contact with (a) scam(s), when compared to respondents residing in *Flanders* (6,6%, χ^2 (2, N=1.036) = 12,76, p<.01). Important to mention here is that the highest portion of those that got victimized or suppose they did, is to be found amongst *Brussels residents* (13,9%). However, respondents residing in Wallonia deviate more from their expected count, and pose therefore the most interesting finding.

Table 6: *Breakdown by residence for scam victimization*

	Flanders	**Wallonia**	**Brussels**	**Victimization total**
Scam victimization - no				
- Percentage within 'no'	55,3%	33,9%	10,8%	100,0%
- Percentage within 'residence'	94,6%	89,3%	89,6%	92,2%
Scam victimization - yes				
- Percentage within 'yes'	**37,0%**	**48,1%**	14,8%	100,0%
- Percentage within 'residence'	**5,4%**	**10,7%**	10,4%	7,8%
Residence total	53,9%	35,0%	11,1%	100,0%
	100,0%	100,0%	100,0%	100,0%

(N=1.036, p = .007)

More than half of the 79 households that became victim of scams in the past year encountered just one incident (53,2%, see Figure 22). A large number of people (34,2%) do not know exactly how many scams they became victim of.

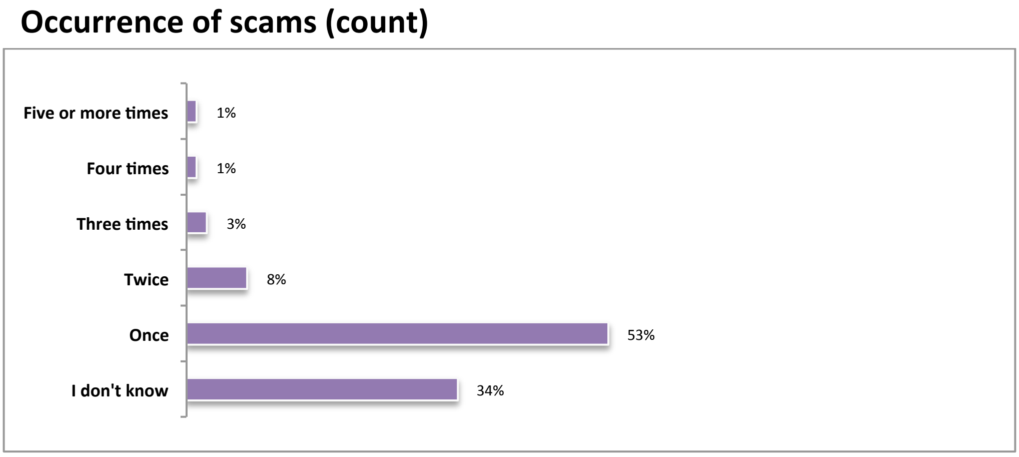


Figure 22: Number of times one became a victim of (a) scam(s) during the past year (N=79)

Of the 51 people that provided valuable information given the ‘when question’, we find that a third of the victims (33,3%) became victim when purchasing a product or service online (see Figure 23) and 14% while selling a product or service online. Again a third (33,3%) do not know during what activity the scam had happened. Two persons (3,9%) indicated that the scam occurred on another occasion, namely while browsing the internet, without further specification.

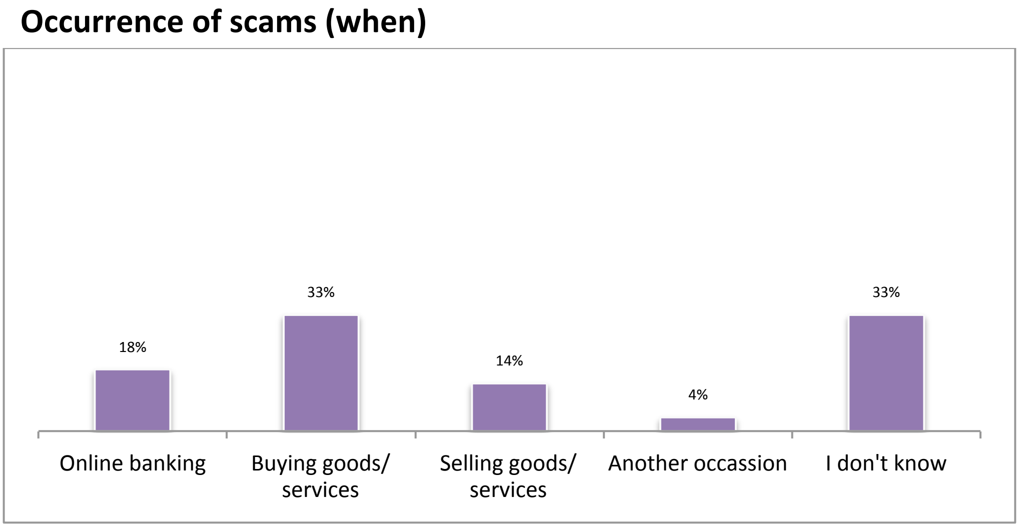


Figure 23: When (during what activity) did the last scam occur? (N= 51)

Crime specific information

22,2% of the scam victims that provided additional, classifiable information considering what kind of attempted or succeeded scam had happened to them or their relatives, encountered the police scam/ransomware (see Figure 24). As the number one reported scam, it is surprising to see how many victims this particular form of cybercrime has made in Belgium. Also, given the fact that ransomware is mentioned both in the ‘virus’ and ‘scam’ categories as one of the most common incidents, it becomes clear that most viruses and scams have a financial motive. Perpetrators construct these deceptions or encodings with an aim for financial gain.

47% of the scams in the respondent group occurred while buying (33%) or selling (14%) goods or services online. As such it should be no surprise that 19,0% of the scam victims that gave classifiable information, became victim in a commercial setting, either as buyer or seller of goods or services. All but one of the 12 vendor/buyer scam victims indicated whether it was the vendor or the buyer that acted as the perpetrator. In 63,6% of the cases, there was a malicious vendor at play. The remaining part (36,4%) identified a buyer with questionable intentions. A quarter (25,0%) of these vendor/buyer victims clearly stated that this happened on a second hand website, and of one person (8,3%), we have reasonable suspicion that this was the case, together adding up to 33,3% of the vendor/buyer scam victims that provided additional information.

Financial fraud appears as the third largest subgroup in our sample (17,5%). The term 'fraud' is used for describing a wide range of (attempted) thefts committed using or involving a payment card, such as a credit card or debit card (credit card fraud), or with the purpose to obtain unauthorized funds from an account, but when it is unclear how exactly this was performed (general financial fraud). Just as surprising as the presence of police ransomware, was the absence of social engineering techniques like telephone scams (3,2%) and mail scams (7,9%, often labeled as 'phishing'). Social engineering within the context of information security, refers to deceiving or the psychological manipulation of people into performing certain actions or divulging confidential information. Then again, certainly not every victim provided information about how exactly the scam was performed.

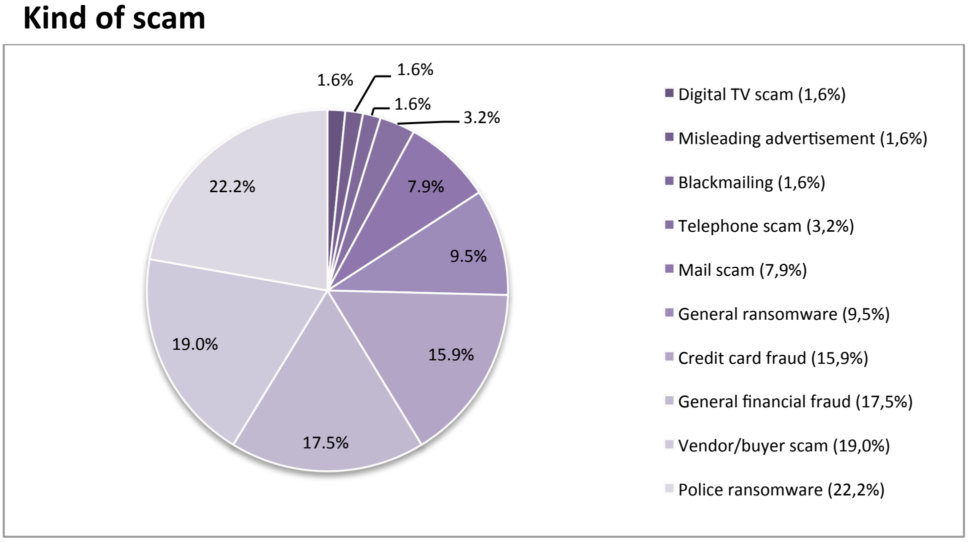


Figure 24: What kind of scam(s) did the respondent or their relative(s) last became victim of?
(classifications distilled from descriptive answers, N=63)

Perceived severity

As mentioned before, **scams** are seen as one of the most severe cybercrime phenomena (*M* = 4,56, *SD* = 0,70). Again, the respondents belonging to Profile 2 – The **overly confident internet user** differ significantly from all of the other profiles (*M* = 4,32, *SD* = 0,85, F (3, 1082) = 8,30, p<.001). They think scams are less serious, especially compared to the **conscious** internet users (Δ 0,34, p<.001).

Reporting

Almost three out of five victims (58,0%) have reported the incident. This indicates that Belgian citizens perceive this type of cybercrimes as more severe (see Figure 25). If reported, it is most often done at the bank/financial institution (25,9%) or with the police (24,7%). Of the thirteen people (16,0%) that reported the incident with another body than those prelisted, five (38,5%) reported the scam with their internet provider, two (15,4%) each with the second hand website, the transactional service company (PayPal and Atos Worldline), and a repair service or the in-store customer support service, and one (7,7%) each with the insurance company and the online retailer (Amazon.com).

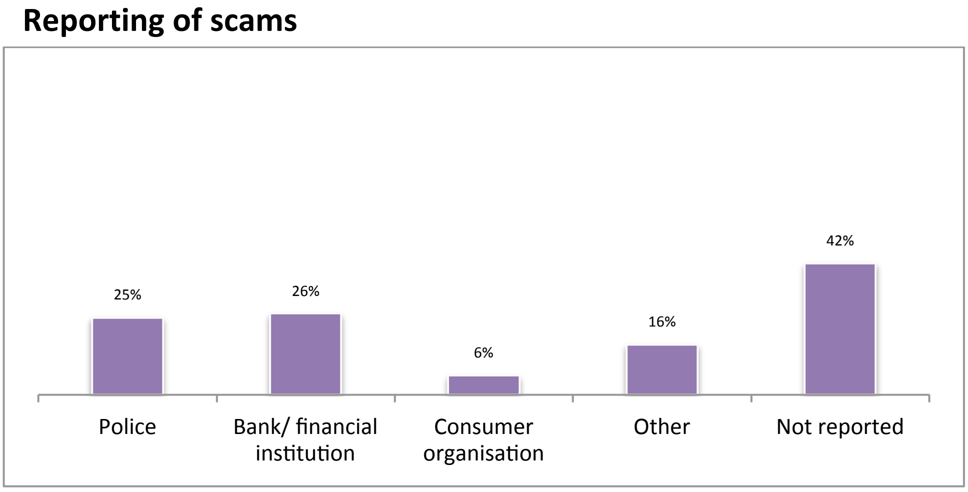


Figure 25: With which body was the last incident reported? (N=81)

2.3 Hacking

Occurrence

More than one out of seventeen people (5,9%) reported that they themselves or one of their relatives encountered 'hacking' or identity theft during the last year (see Figure 14). This number rises to 10,5% (more than one in ten people) when taking into account the people that suspect this to have happened (see Figure 15). Of the people that were hacked, or know about a hacking in their immediate surroundings, 47,0% (26,5% within the 'supposedly yes' group) is certain that they themselves became a victim, 31,8% (17,9%) believe that someone else in their family became a victim, and 21,2% (12,0%) that both they themselves and someone else in their family became a victim.

With respect to our profiles, we find that 13% of the respondents belonging to Profile 1 - The **conscious internet users** and 14,1% of the respondents belonging to Profile 4 - The **resolved internet users** at least suspect to have been victimized by hackers. This is almost double the percentage of the victims within Profile 2 - The **overly confident internet users** (7,5%) and Profile 3 - The **inexperienced internet users** (7,8%), χ^2 (3, N=1.082) = 9,32, p<.05).

Again, there is a clear difference noticeable according to the place where one resides (see Table 7). This time, however, the *Brussels residents* seem to encounter hacking more than other Belgians do. Almost one out of seven (14,8%) people that reside in *Brussels* report to have become a victim of hacking, or know someone in their close environment who did, in the past year (χ^2 (2, N=1.035) = 27,98, p<.001). A significant number, when compared to respondents residing in *Wallonia* (8,0%) and certainly *Flanders* (2,9%). Respondents residing in *Wallonia* represent almost half (46,8%) the number of people that were victimized in the last year, almost double the number of those that live in *Flanders*. However, they do not deviate from their expected count as much as *Brussels residents* do. This (at first glance contradictory) finding is explained by more than threefold the number of people who reside in *Wallonia*, compared to *Brussels* (see Figure 3). This pattern is confirmed when also taking into account those that suspect having been a victim of hacking (χ^2 (2, N=1.035) = 17,65, p<.001).

Table 7: *Breakdown by residence for hacking victimization*

	Flanders	Wallonia	Brussels	Victimization total
Hacking victimization - no				
- Percentage within 'no'	55,6%	34,3%	10,1%	100,0%
- Percentage within 'residence'	97,1%	92,0%	85,2%	94,0%
Hacking victimization - yes				
- Percentage within 'yes'	**25,8%**	46,8%	**27,4%**	100,0%
- Percentage within 'residence'	**2,9%**	8,0%	**14,8%**	6,0%
Residence total	53,8%	35,1%	11,1%	100,0%
	100,0%	100,0%	100,0%	100,0%

(N=1.035, p = .000)

Almost half of the 65 households that became victim of hacking in the past 12 months, encountered just one incident (49,2%, see Figure 26). Again, a large number of people (38,5%) do not know exactly how many hacks they became victim of.

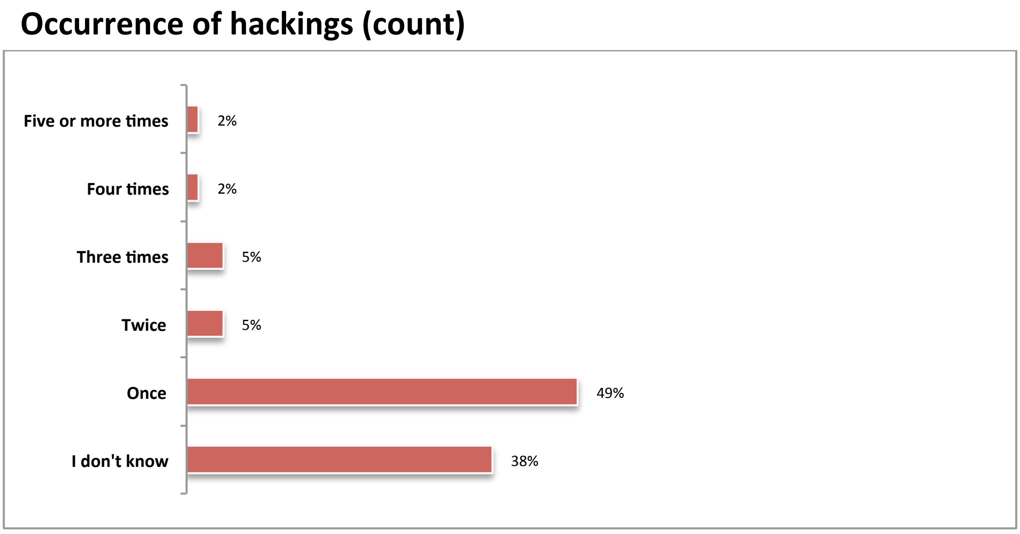


Figure 26: Number of times one became a victim of hacking(s) during the past year (N=65)

Crime specific information

When asking more in detail about what happened, almost half the victims (41,5%) stated that their e-mail account was broken or unlawfully logged into (see Figure 27). This group is followed by quite a few people (almost one out of four victims or 23,1%) that do not even know what got hacked particularly and a group that believes their social media account was hacked (18,5% or almost one in five victims). The latter should not be a surprise, given the proliferation of social media accounts and associated activity in recent years (Digimeter, 2014). In four cases (6,2%), something else than the prelisted categories was hacked: a banking account (followed by credit card fraud), a chat account, an online gaming account (World of Warcraft), and a phone account (followed by having messages sent in the person's name), each accounting for 1,5% of the hacked victims.

The open, descriptive question did not yield many additional insights, besides the following: two persons (3,1%) clearly stated their mail account was hacked with the purpose of sending out spam to their contact list; one person (1,5%) stated that he/she became a victim of hacking by a competitor within the economic market; one person believed his digibox/digicorder (digital television receiver) was hacked and the perpetuator kept ordering pay movies; and someone active in the financial industry claimed that the banking web module 'Isabel' (or at least his account) was hacked with deprived currency as a result.

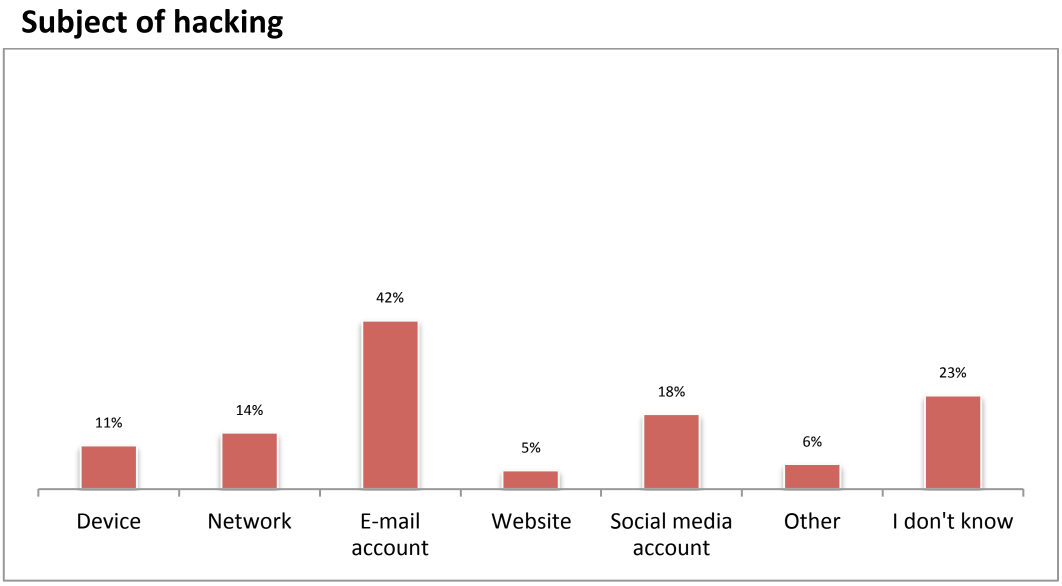


Figure 27: What was broken or unlawfully logged into the last time you encountered hacking? (N=65)

Perceived severity

As mentioned before, **hacking** is seen as one of the most severe phenomena (*M* = 4,59*, SD* = 0,66). Again, the respondents belonging to Profile 2 – The **overly confident internet users** differ significantly from all of the other profiles (*M* = 4,40, *SD* = 0,81, F (3, 1082) = 6,52, p<.001). They think scams are less serious, especially compared to the respondents belonging to Profile 1 – The **conscious internet users** (Δ 0,28, p<.001).

Reporting

Slightly more than two out of five victims (43,1%) reported the hacking incident, making this form of cybercrime better reported than viruses, but less than scams (see Figure 28). A possible explanation for this finding is the fact that there is not always a financial loss accompanying this crime, and consequently people do not feel the need to report when being victimized. When reported, it is most often done with law enforcement (15,4%) and the company behind the social media or website (e.g. Facebook or Skyrock). Seven people indicated they reported the incident with another body than those prelisted, including their financial institution or transactional service company (Visa and Worldline, 3,1% of hack victims), and the online retailer (Amazon), game developer (Blizzard), digital television provider (Belgacom), e-mail provider and Microsoft, each accounting for 1,5% separately.

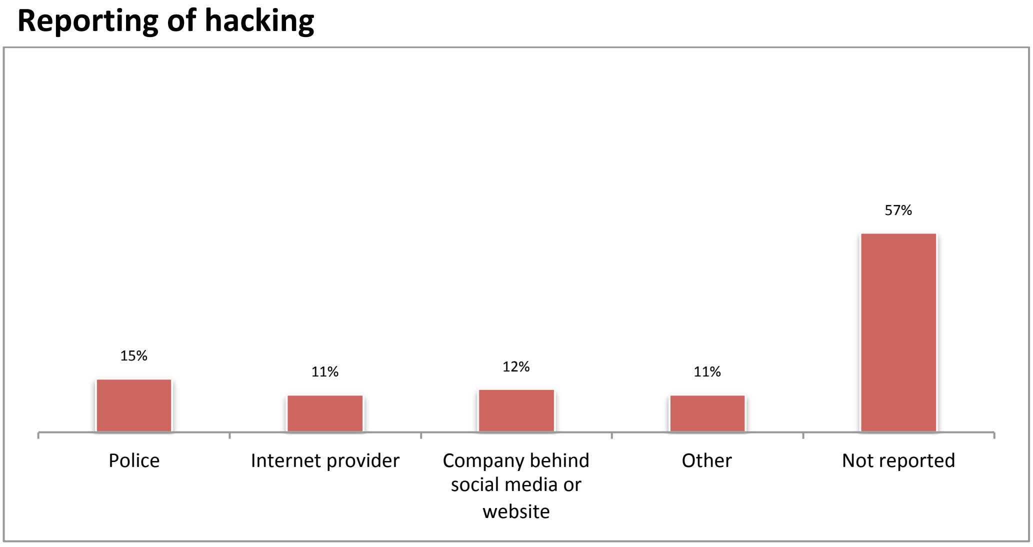


Figure 28: With which body was the last incident reported? (N=65)

2.4 Governmental surveillance and corporate surveillance

Occurrence

The Belgian citizens are least certain about having encountered surveillance by governmental institutions in the past twelve months (see Figure 14). Only 4,8% is certain about having their, or their relatives' personal data processed without consent and/or prior knowledge by the government, making it the least reported cybercrime phenomenon in our survey. This finding stands in stark contrast with more than double the proportion of people (10,7%) who believe a private company did this for commercial reasons. Both types of surveillance count the most people that suspect the phenomenon to have occurred but do not know for sure, respectively 20,0% for surveillance by a domestic or foreign government and 28,7% for corporate surveillance, and the highest number of people that do not know whether or not this has occurred (respectively 39,6% and 30,4%, see Figure 15). These findings suggest that of all six questioned phenomena, both governmental surveillance and corporate surveillance are considered to be the most obscure cybercrime types.

Most 'victims' of governmental surveillance believe that both they themselves and someone else of their family were scrutinized (52,8% or 10,2% within the 'supposedly yes' group), followed by 35,8% (6,9%) who believe that only they themselves, and 11,3% (2,2%) that someone else in the family were/was under governmental surveillance during the past year. This contrasts with the finding that corporate surveillance affects a majority mere personally (57,1% or 15,5%), followed by 35,3% (9,6%) of the 'victims' who believe that both their own personal data and that of relatives was collected and/or traded by private companies, and a small 7,6% (2,1%) that stated that someone else in the family encountered corporate surveillance.

With respect to our profiles, we find that 30,1% of the respondents belonging to Profile 1 – The **conscious internet users** at least suspect that government agencies track their whereabouts, while the respondents of Profile 2 - The **overly confident internet users** form their counterpart with only 16,4% (χ^2 (3, N=1.081) = 14,73, p<.01) of them that believes so. For the respondents of the Profiles 3

(The **inexperienced internet users)** and 4 (The **resolved internet users)**, these percentages are respectively 20,6% and 26,6%.

Younger people are more convinced about practices of governmental surveillance to be happening. The *youngest age category (18 to 34 year olds)* represent almost half (48,9%) the number of people that are sure the government keeps an eye on them and/or their family (see Table 8, χ^2 (4, N=1.034) = 16,13, p<.01). Despite their preponderance in the population and our sample (27,6% of total respondents is younger than 35, see Figure 2), this is the largest deviation found in our sample, with respect to both variables. Reversely, only 1,0% of the *elderly (65+)* is convinced governmental surveillance takes place in their own and/or their family's personal lives. Higher educated people seem to be less certain about the fact that they are subject to governmental surveillance: not one person with a *(post-)graduate/Master's degree* (0,0%) indicated they encountered this phenomenon (χ^2 (7, N=1.031) = 14,35, p<.05, caveat: expected count < 5 (4,8)). Adding the people that suspect government surveillance to have happened, we find further evidence for the above-mentioned age divide (χ^2 (4, N=1.034) = 17,51, p<.01). Also worth mentioning, is that more than a third (36,9%) of those *incapacitated for work or on long-term sick leave* suspects to be monitored by the government (χ^2 (10, N=1.032) = 20,55, p<.05).

Table 8: *Breakdown by age category for governmental surveillance victimization*

	18-34	35-44	45-54	55-64	65+	Victimization total
Gov. surveillance victim. - no						
- Percentage within 'no'	26,6%	15,0%	24,8%	14,1%	19,6%	100,0%
- Percentage within 'age category'	92,3%	94,9%	95,7%	98,6%	99,0%	95,6%
Gov. surveillance victim. - yes						
- Percentage within 'yes'	**48,9%**	17,8%	24,4%	4,4%	**4,4%**	100,0%
- Percentage within 'age category'	**7,7%**	5,1%	4,3%	1,4%	**1,0%**	4,4%
Age category total	27,6%	15,1%	24,8%	13,6%	19,0%	100,0%
	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

(N=1.034, p = .003)

Respondents belonging to Profile 1 – The **conscious internet users** suspect more than the respondents belonging to Profile 2 – The **overly confident internet users** that their personal data was used for commercial reasons: respectively 48% and 25,3% of these profiles suspect or are certain this was the case (χ^2 (3, N=1.083) = 24,31, p<.001). This difference between both profiles is again most apparent when looking only at those who suspect this phenomenon to have happened in the past twelve months.

Brussels residents seem to be more convinced of the fact that their personal data is being traded by private companies, with almost a fifth (17,4%) of them having indicated this is the case, compared to 9,9% of the people residing in *Flanders* and 8,0% of the people residing in *Wallonia* (χ^2 (2, N=1.036) = 8,59, p<.05). As is the case with government surveillance, young adults seem to believe they encountered corporate surveillance more than elderly do (see Table 9). The group that is certain they have been the subject of corporate surveillance in the past year, consists of almost four times as many *18-34* than *65+ year olds* (respectively 38,5% and 10,6%, χ^2 (4, N=1.036) = 16,08, <.01). Again, this age divide is confirmed when also taking into account those that suspect this to have happened. Opposed to our finding with government surveillance, more higher educated respondents, compared to other educational levels, at least suppose they have been the subject of corporate surveillance: half (49,1%) of the (*post-)graduate/Master degrees* (χ² (7, N=1.033) = 16,14, p<.05).

Table 9: *Breakdown by age category for corporate surveillance victimization*

	18-34	35-44	45-54	55-64	65+	Victimization total
Corp. surveillance victim. - no						
- Percentage within 'no'	26,3%	15,5%	24,0%	14,4%	19,8%	100,0%
- Percentage within 'age category'	86,0%	91,7%	87,2%	95,0%	94,4%	90,0%
Corp. surveillance victim. - yes						
- Percentage within 'yes'	**38,5%**	12,5%	31,7%	6,7%	**10,6%**	100,0%
- Percentage within 'age category'	**14,0%**	8,3%	12,8%	5,0%	**5,6%**	10,0%
Age category total	27,5%	15,2%	24,8%	13,6%	18,9%	100,0%
	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

(N=1.036, p = .003)

A convincing majority of the respondents that believe they were monitored by the government do not know how many times this has happened in the past year (74,0%) (see Figure 29). The same can be said, but to a lesser extent, about the occurrence of corporate surveillance (62,8%, see Figure 30). What is remarkable here is that almost a quarter (23,9%) of those who have experienced corporate surveillance, believe this to have happened five times or more during the past year. These people are likely to have the impression that their personal data has market value and is quite often collected and traded on the market place.

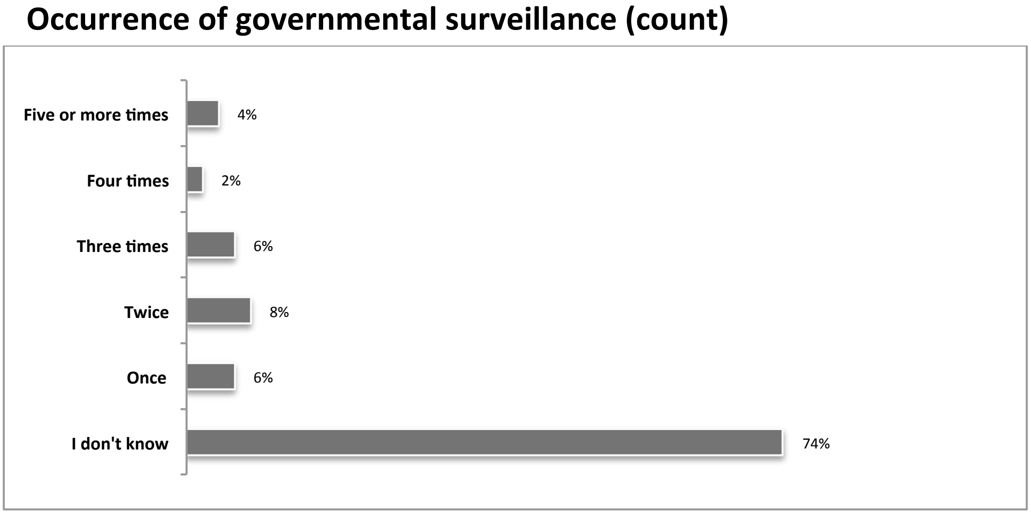


Figure 29: Number of times one has encountered governmental surveillance during the past year (N=50)

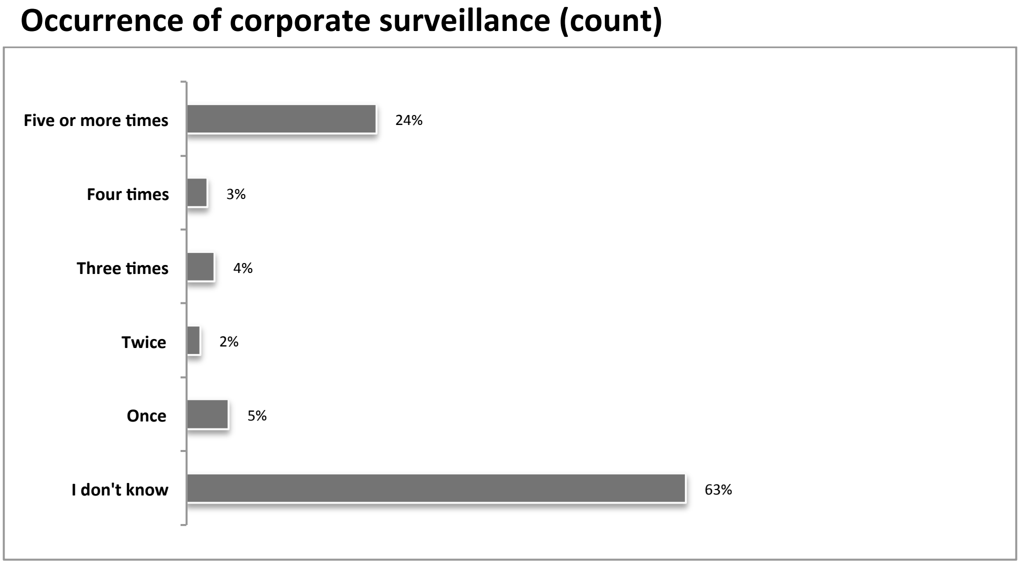


Figure 30: Number of times one has encountered corporate surveillance during the past year (N=113)

Crime specific information

When asking to recall the last time such an incident occurred, the results differ quite significantly between both acting parties considering what exactly happened (see figures 31 and 32). People that encountered governmental surveillance remain mostly in doubt and do not know exactly what happened (64,0%), while those who experienced corporate surveillance clearly indicated they did not gave explicit permission to do so (40,2%) or they did not have prior knowledge that their personal data was used for commercial purposes (37,5%). When people are aware of the intrusion into their private lives by government agencies, they most often claim not having given permission to do so (24,0%).

When looking at other given grounds for declaring the use of data an act of intrusion of the personal sphere, we find for governmental surveillance that one person stated the government kept an eye on her ever since she was suspected of terrorism, one person declared his internet behavior is under constant surveillance, and a last person could not connect with his ID card, each accounting for 2,0% of scam victims. Since it is unclear whether or not these answers can reside under one or more of the prelisted answering categories, they were not recoded. The same goes for corporate surveillance, where nine people (8,0%) described in general the use of their personal data for maximizing financial profit, without specifying what exactly formed the ground for calling it an intrusion. Interestingly, two persons (1,8%) focused attention on the terms and conditions of use: many websites ‘force’ visitors to accept cookies, for example by an otherwise reduced usability. Lastly, three respondents (2,7%) indicated they received a lots of spam while asking themselves how these companies got their mail address, and one person (0,9%) was contacted numerous times by unknown companies over the telephone.

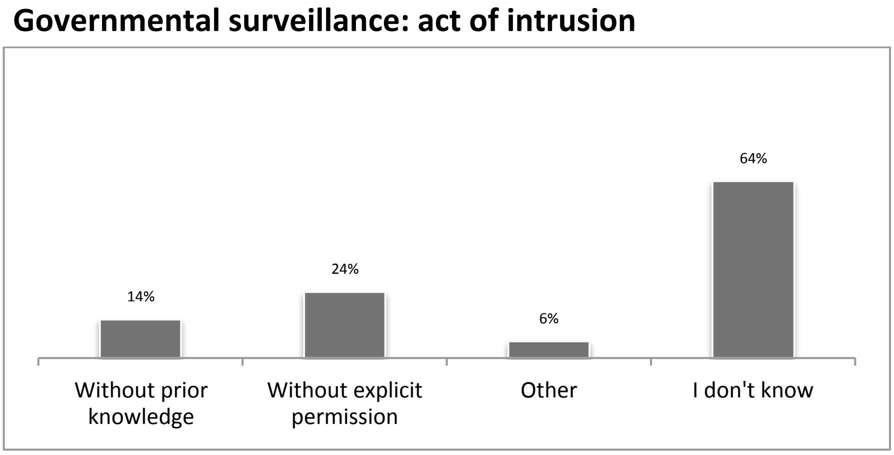

Governmental surveillance: act of intrusion

Figure 31: What exactly happened the last time you encountered governmental surveillance? (N=50)

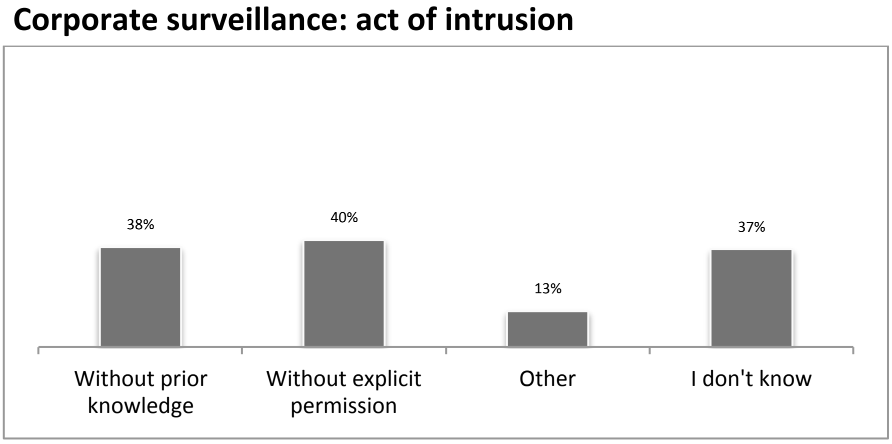

Corporate surveillance: act of intrusion

Figure 32: What exactly happened the last time you encountered monitoring by private companies? (N=112)

In analyzing the answers on the descriptive, open questions, only one person (2,1%) left no doubt and clearly formulated that people are inevitable being tracked online by foreign intelligence agencies. Besides this exception, we found no indication of any concern whatsoever about mass surveillance in people's perception. This finding is very interesting in a sense that it contradicts increased awareness about mass surveillance since the Snowden revelations. We did find many different descriptions in which personal data is used in a commercial way (corporate surveillance), too many, however, to distil distinct, meaningful subcategories. Worth mentioning is the fact that 13,3% of the people that encountered corporate surveillance received a large amount of spam (mail), whether or not personalized, 7,1% were called numerous times by telemarketers, and one person (0,9%) indicated that his address and contact details had been published publicly.

Perceived severity

As mentioned before, **corporate surveillance** and especially **governmental surveillance** are perceived as one of the least serious internet crimes (respectively *M* = 4,23, *SD* = 0,86, and *M* = 3,93, *SD* = 0,93). User profiles did not differ significantly concerning monitoring by governmental surveillance, while there are some differences for corporate surveillance. The respondents belonging to Profile 2 - The **overly confident internet user** differ significantly from those belonging to Profile 1 (The conscious internet users) and Profile 3 (The inexperienced internet users) (*M* = 4,03, *SD* = 0,94, F (3, 1082) = 5,06, p<.01). They think corporate surveillance is less serious, especially compared to the respondents belonging to Profile 1 - The **conscious internet** users (Δ 0,31, p<.01).

Reporting

Furthermore, it should be no surprise that both surveillance by government agencies and surveillance by private entities is almost never reported: respectively 91,6% (governmental surveillance) and 90,3% (corporate surveillance) of the respondents state they did not report the last incident with any body (see Figures 33 and 34). However, almost one in ten 'victims' (8,8%) did report the incident with the private company they held responsible for the intrusion.

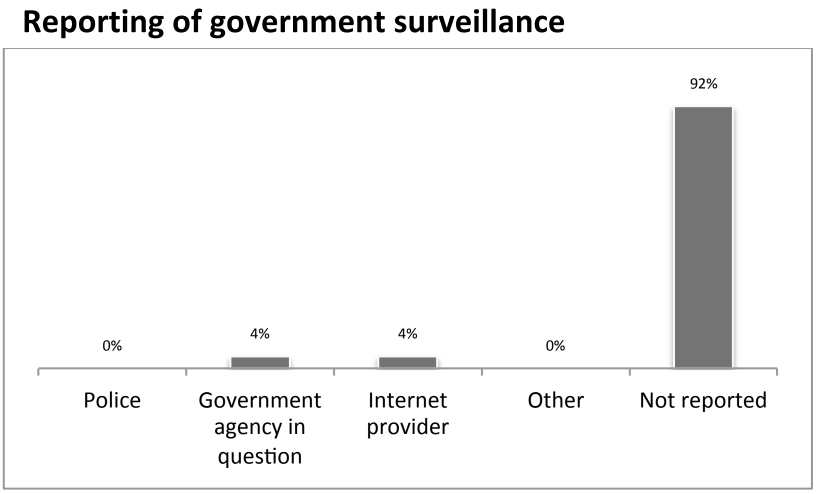


Figure 33: With which body was the last incident reported? (N=48)

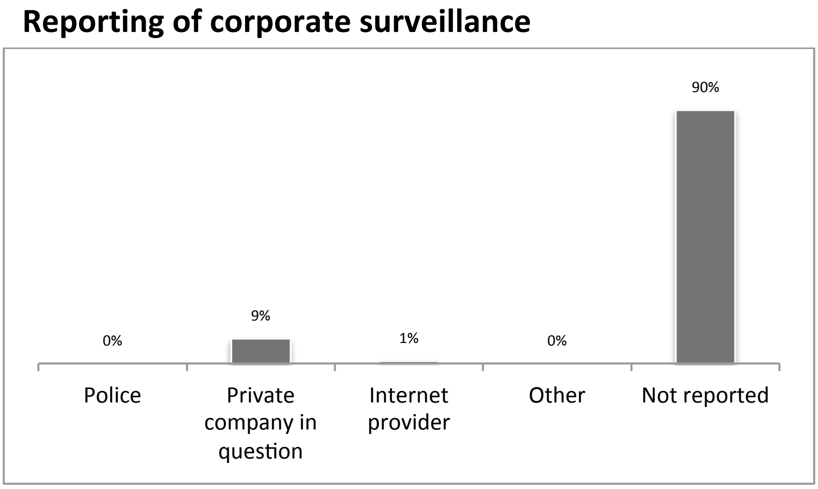


Figure 34: With which body was the last incident reported? (N=113)

2.5 Unwanted content and/or behavior

Occurrence

Almost one out of ten people (9,7%) have witnessed unsolicited content and/or behavior on the internet, or have knowledge about a family member having experienced this (see Figure 14). Interestingly, this number rises to 18,0% when taking into account those respondents that suspect this to have happened (see Figure 15). One would expect people to know for sure whether or not they came in contact with unwanted content and/or behavior, but apparently there is some doubt surrounding this phenomenon: 17,7% state they do not know if they were victimized in the last year. When victimized, it was mostly the respondent him-/herself (44,4% or 24,0% within the 'supposedly yes' group), followed by both the respondent and his/her relative(s) (32,4% or 17,5%) and someone else of the family (23,1% or 12,5%).

Respondents belonging to Profile 1 – The **conscious internet users** are more certain than other profiles that they encountered such unwanted content and/or behavior (12,7%). Though, we have to acknowledge this time it is not the Profile 2 (The **overly confident internet users)** that forms its counterpart, but Profile 3 (The **inexperienced internet users)**, with only 6,8% of them having witnessed such content/behavior. Adding those that supposed to have been victimized, the contrast between both profiles remains: 22,8% of the respondents belonging to Profile 1 – The conscious internet users versus 14,6% of the respondents belonging to Profile 3 (The inexperienced users) at least suspect to have encountered unwanted content and/or behavior (χ^2 (3, N=1.083) = 12,85, p<.01). However, this time the respondents belonging to Profile 2 – The **overly confident internet users** represent the lowest victimization rate: only 11,6% of them indicated they were at least presumably victimized.

More *men* than *women* are convinced of the fact they have encountered such content/behavior. Almost double the number of *men* (11,8%) are certain this to have happened, compared to *women* (6,9%, χ^2 (1, N=1.036) = 7,11, p<.01). Within the 'supposedly yes' group, men represent 61,0%, while women only 39,0% (χ^2 (1, N=1.036) = 10,67, p<.01). Only 5,4% of the respondents residing in *Flanders* reported to have witnessed unwanted content and/or behavior, while (almost) triple the portion of the respondents residing in *Wallonia* (13,2%) or *Brussels residents* do (see Table 10, χ^2 (2, N=1.036) = 23,77, p<.001). Add the ones that suppose such a thing to have happened, and the respondents residing in Wallonia make up more than half (50,5%) of their number (χ^2 (2, N=1.036) = 36,77, p<.001). Further, more than one out of four (25,2%) of the *Brussels residents* at least suspect to have been a victim of such a cybercrime, compared to only 10,9% of respondents residing in Flanders. Looking solely at the ones that suppose they encountered unwanted content and/or behavior, again the respondents residing in Wallonia account for the largest share with 51,8% of the respondents that suspect such a thing to have happened (χ^2 (2, N=1.036) = 12,63, p<.01).

Table 10: *Breakdown by residence for unwanted content and/or behavior victimization*

	Flanders	Wallonia	Brussels	Victimization total
Unwanted cont./beh. victim. - no				
- Percentage within 'no'	56,2%	33,5%	10,2%	100,0%
- Percentage within 'residence'	94,6%	86,8%	83,5%	90,6%
Unwanted cont./beh. victim. - yes				
- Percentage within 'yes'	**30,9%**	**49,5%**	**19,6%**	100,0%
- Percentage within 'residence'	**5,4%**	**13,2%**	**16,5%**	9,4%
Residence total	53,9%	35,0%	11,1%	100,0%
	100,0%	100,0%	100,0%	100,0%

(N=1.036, p = .000)

Younger people declare significantly more than older people to have encountered unwanted content/behavior: respectively 13,7% and 6,1% of the *youngest (18-34)* and *oldest (65+) age category* did (see Table 11, χ^2 (4, N=1.036) = 9,87, p<.05). This was again confirmed by the 'supposedly yes' results (χ^2 (4, N=1.036) = 10,83, p<.05).

Table 11: *Breakdown by age category for unwanted content and/or behavior*

	18-34	35-44	45-54	55-64	65+	Victimization total
Unwanted cont./beh. victim. - no						
- Percentage within 'no'	26,2%	15,1%	25,2%	13,8%	19,6%	100,0%
- Percentage within 'age category'	86,3%	90,4%	92,2%	92,2%	93,9%	90,6%
Unwanted cont./beh. victim. - yes						
- Percentage within 'yes'	**40,2%**	15,5%	20,6%	11,3%	**12,4%**	100,0%
- Percentage within 'age category'	**13,7%**	9,6%	7,8%	7,8%	**6,1%**	9,4%
Age category total	27,5%	15,2%	24,8%	13,6%	18,9%	100,0%
	100,0%	100,0%	100,0%	100,0%	100,0%	100,0%

(N=1.036, p = .043)

Most victims or close relatives of victims indicate they do not know how many times unwanted content and/or behavior appeared or was demonstrated in the last year (39,2%, see Figure 35). On the one hand, almost a quarter of the victims (24,9%) believe it has happened only once, which suggests it to be a rare phenomenon. On the other hand, however, quite a few people (20,6% or more than one in five) believe it to have happened five or more times, stating the contrary.

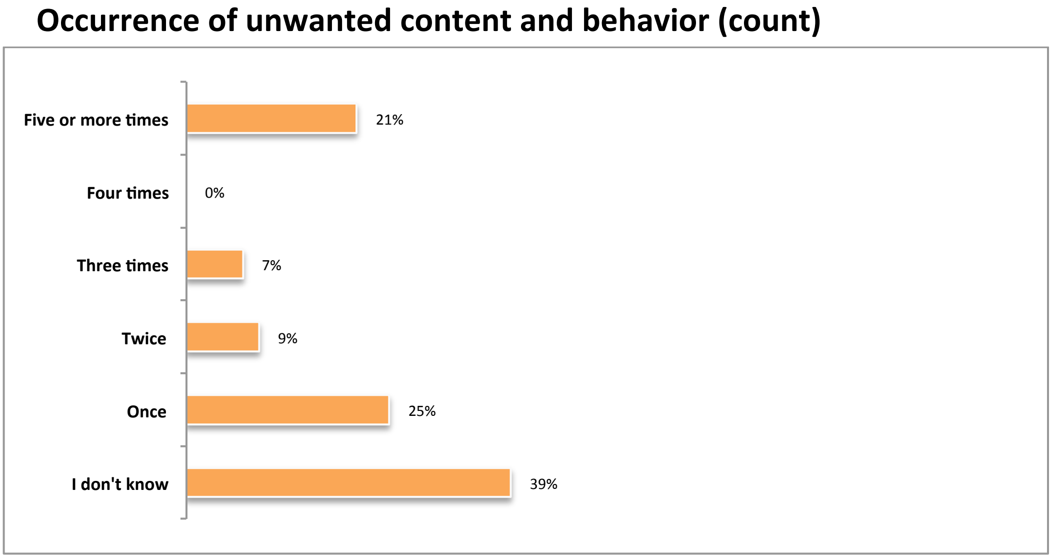


Figure 35: Number of times one encountered unwanted content and/or behavior during the past year (N=102)

Crime specific information

The highest category of unwanted content victims got in touch with, is unwanted content of a sexual nature (42,7% or more than two in five, see Figure 36). All other categories are more or less equally represented, regardless of the fact that it concerns (visual) content or behavior. The 'other' answering category consists entirely of people that indicated they encountered unsolicited advertisement. This category should be considered an underestimation of the true number of people that encountered unwanted advertisement, since it is very likely that many people that received advertisements or spam within the 'corporate surveillance' category consider these messages as unwanted content or even behavior. A better estimation of this unwanted advertisement is obtained when analysing the descriptive, open question. Here, 25,0% of the victims indicated they were annoyed by frequently appearing advertisement, in the form of spam mail or pop-up windows.

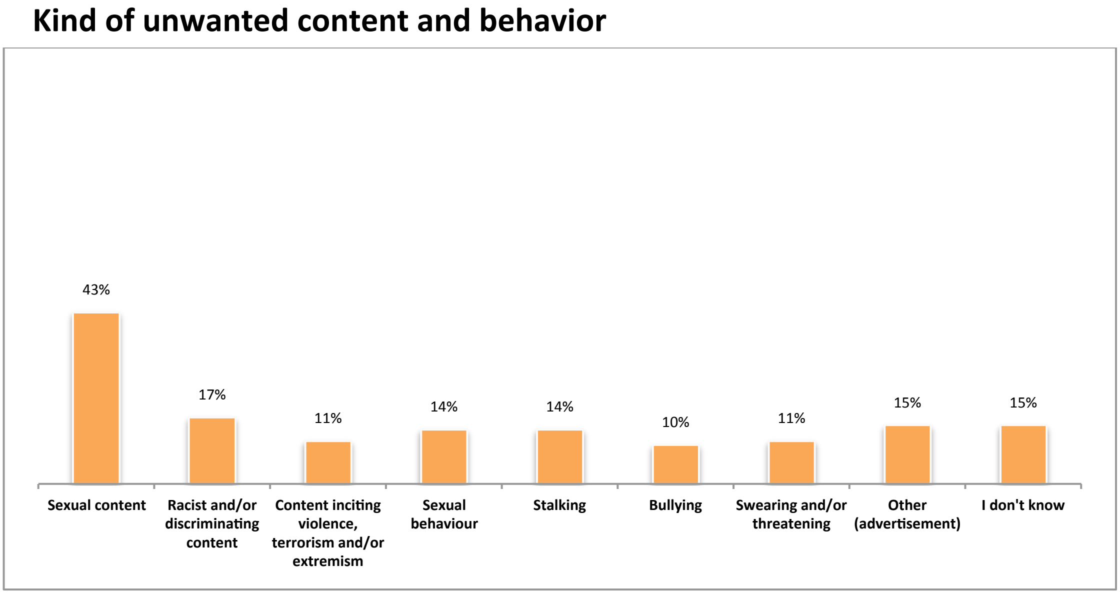


Figure 36: What did you get in touch with the last time? (N=103)

Perceived severity

As mentioned before, unwanted content and/or behavior has an average perceived seriousness (*M* = 4,29, *SD* = 0,90). The respondents belonging to Profile 2 – The **overly confident internet users** perceives this crime significantly less serious than the respondents belonging to Profile 1 - The **conscious internet users** (*M* = 4,05, *SD* = 1,05 vs *M* = 4,43, *SD* = 0,81, F (3, 1082) = 6,42, p<.001).

Reporting

A large majority (77,8% or almost four in five) of victims do not report with anyone when having encountered unwanted content and/or behavior (see Figure 37). If reported, it is most often done with the company behind the social media platform or the website on which the crime occurred (9,6% or almost one in ten victims). Four victims (3,8%) reported the last incident with another body than those prelisted: 1,9% probably by means of an automatically generated problem report, sent to the antivirus and operating system company (in casu respectively Avast free antivirus software and Microsoft), 1,0% with the telecom provider and another 1,0% with the justice department. All open questions considered, 1,9% of the victims indicated they had to go to court to stop the bullying, swearing, threatening and unwanted content of a sexual and racist nature.

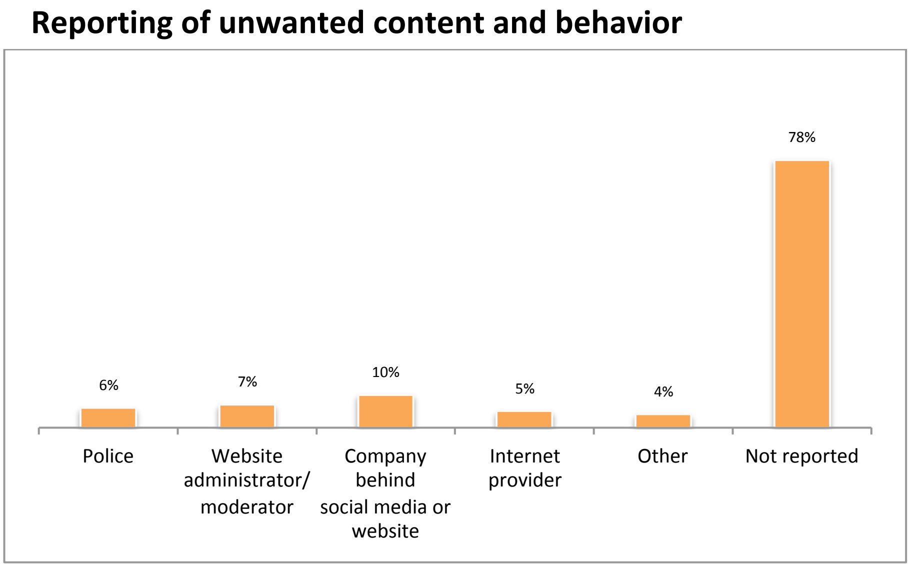


Figure 37: With which body was the last incident reported? (N=104)

2.6 Financial impact

With regard to the financial impact of cybercrime, many people refrain from estimating the financial loss they have suffered as a result of these crimes (see Figure 38). In this respect it is important to mention that not only the victims (or their relatives) of the respective crimes got to see this question, but also those that suspect to have been victimized. For example, of the people that suspect to have become a victim of viruses, 27,1% do not know what financial damage he/she suffered, compared to only 6,2% of those that are certain they were victimized (χ^2 (6, N=1.110) = 286,28, p<.001).

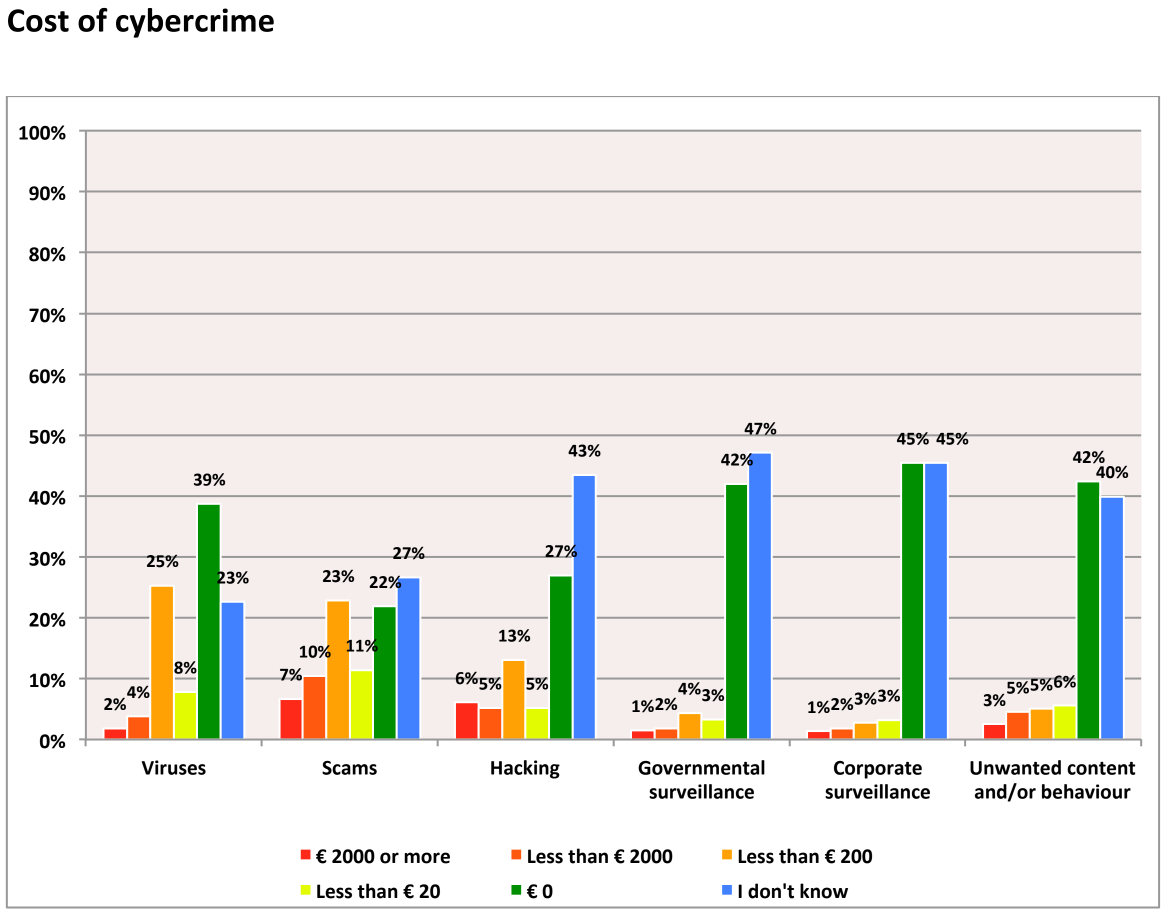


Figure 38: estimated financial impact of cybercrime , including the cost of incurred damage, protective measures and/or repairing (*Viruses*: N=447; *Scams*: N=105; *Hacking*: N=115; *Governmental surveillance*: N=274; *Corporate surveillance*: N=436; *Unwanted content and/or behavior*: N=198)

It is indeed a difficult - if not impossible – exercise to calculate this, since not all adverse effects can be easily monetized. Consider losses like the time and effort to reset account credentials, the distress suffered by victims, lost attention and bandwidth caused by spam, etc. (Anderson et al., 2013). Furthermore, it is important to note that losses are often distributed between different stakeholders (Rughiniş & Rughiniş, 2014). For example, in the case of a hacked bank account, citizens are often protected from financial risks by arrangements that transfer financial losses to corporate actors. This causes certain costs to be hidden, appearing more like a minor inconvenience for the victim. People were least certain about the suffered financial damage of ‘hacking’, ‘surveillance by government’, ‘corporate surveillance’ and ‘unwanted content and/or behavior’, with 40% or more having indicated to not know (see Figure 38). This should come as no surprise, given the fact that these phenomena often result in an intangible impact, and financial implications are certainly not always clear or measureable.

However, certain security measures, suffered damages or reparations, have non-negligible costs, and most people did estimate the financial loss they suffered from cybercrime. Scams appear to result in greater financial losses than other crimes do, as is expected given the financial motives behind these crimes. More than one in ten (10,5%) scam victims lost a considerable amount of money due to scams: somewhere in the €200 - €2.000 range. Compared to other crimes, the highest number of people (6,7%) reported to have lost even more than €2.000 as a result of or by preventing from getting scammed. An almost equal number of (supposed) hacking victims (6,1%) believe to have suffered losses in the same order of magnitude. Viruses most often seem to result in either no cost at all (38,7%) or a lower cost (< €200, 25,3%).

There appears to be a discrepancy between our internet user profiles, considering the financial losses resulting from **unwanted content and/or behavior** (Kruskal-Wallis test: χ^2 (3, N=113) = 8,28, p<.05). Looking at the frequency tables, we learn that respondents belonging to Profile 2 – The *overly confident internet users* suffer significantly greater losses than other profiles do, with regard to this cybercrime. Only 2,1% of these users reported no financial damage, compared to 10,4% of the respondents belonging to Profile 1 – The *conscious internet users* (χ^2 (18, N=1.081) = 33,40, p<.05). This is rather surprising, since the respondents belonging to Profile 2 – The overly confident internet users are less likely to have become a victim of unwanted content and/or behavior in the past 12 months (vide supra). These users rarely encounter unsolicited content and/or behavior online, but when they do, they suffer greater financial losses.

Men suffer more financial damages as a result of **scams** and **hacking** than *women* do (respective Mann-Whitney tests: U (N=74) = 493,00, p<.05 and U (N=61) = 317,00, p<.05). There is a significant difference between the *Brussels residents*, residents from *Wallonia* and *Flanders*, considering the financial losses resulting from **viruses**, **governmental surveillance**, **corporate surveillance** and **unwanted content and/or behavior** (respective Kruskal-Wallis tests: χ^2 (2, N=313) = 14,32, p<.01; χ^2 (2, N=134) = 19,76, p<.001; χ^2 (2, N=220) = 13,26, p<.01; χ^2 (2, N=106) = 6,16, p<.05). Looking more into detail, residents from Brussels seem to have the greatest monetary losses, followed by respondents residing in Wallonia. To illustrate: respondents residing in Flanders make up respectively 67,9% and 64,8% of those that suffered no financial loss from governmental surveillance (χ^2 (12, N=1.034) = 24,73, p<.05) and corporate surveillance (χ^2 (12, N=1.036) = 37,06, p<.001). Compared to other professions, people in *management or executive functions* are more convinced to have suffered no financial damage as a result of **corporate surveillance**, as we learn from a majority of them (32,6%, χ^2 (60, N=1.034) = 88,11, p<.05).

2.7 Conclusion

In this section we have reported about cybercrime victimization. We have analyzed whether or not our respondents have been the victims of different types of cybercrime, i.e. viruses; scams; hacking; governmental surveillance; corporate surveillance; and unwanted content and/or behavior. From these cybercrime types, most respondents have been the victims of viruses. On the other hand, scams and hacking seem to be the cybercrime types of which our respondents have been least the victims. Per cybercrime time, we have included a detailed discussion about occurrence, perceived severity, and whether or not the victims have reported the encounter of this cybercrime.

In addition to this, this section also has focused on the financial impact of cybercrime. In order to do so, we have asked the respondents to estimate the (financial) costs that have occurred because of being the victim of the different types of cybercrime. Our results indicate that scams and hacking result in larger costs, while for other categories respondents have more difficulties to make this estimation.

3 Risk perception monitoring tool

Public authorities can and should inform the public about their vulnerability to cybercrime, the probability of becoming victimized, the severity of cybercrime and what they can do about it. Following the Protection Motivation Theory (PMT) receiving such information can influence the public's attitude, and consequently their intention to adopt protective measures.

In what follows we will investigate to what extent PMT holds true in the context of internet security measures. Secondly, we will identify whether being informed about online risks and how to avoid them is positively associated with the public's intention to adopt security measures concerning cybercrime. If these two hypotheses are affirmed, it is justified to use the PMT model as the fundament of an effective risk communication strategy. In this regard, a final aim is to investigate the respondents' scores on the different variables of the PMT-model, and compare them for the different user profiles. Regression models are used to determine to what extent the PMT variables are associated with intention for the four profiles. As such, these can be approached with differentiated communication strategies, allowing a more tailored and thus effective campaign.

3.1 PMT in an internet security context

Before any analysis was made, all scales used to measure the different PMT constructs were tested for their intern reliability. Both *perceived severity* (Cronbach's alpha = .85), *perceived vulnerability* (Cronbach's alpha = .77), *self-efficacy* (Cronbach's alpha = .75), *subjective norm* (Cronbach's alpha = .86) and *intentions to perform security related behavior* (Cronbach's alpha = .83) were internally consistent.

After deleting one item from *attitude towards security related behavior*, the Cronbach's alpha for this scale increased from 0,67 to 0,71. *Response efficacy* had a Cronbach's alpha of 0,64. This could not be increased by deleting an item, so was decided to use this scale anyway.

A linear multiple regression analysis was conducted for all user profiles. All above-mentioned variables were included in the model to define whether these variables were associated with the outcome measure *intention to adopt internet security measures*. In order to control for gender, age and education, these variables were included subsequently. Finally we added the variable *user profile*.

The model proves to be significant, F (8, 1035)= 68,81, p<.001, and has a moderate explanatory power (R^2= .34). All the variables of the PMT model are significant predictors of *intention to adopt internet security measures*, of which subjective norm is the strongest (*b**= .34, p<.001) and response efficacy the weakest (*b**= .10, p<.01). When controlling for socio-demographic variables, only gender seems to have a significant association with our outcome variable. Males show a lower intention (*b**= -.08, p<.01) to adopt security measures than women. Although significant, this association is very weak. When taking the user profile groups into account, Profile 1 (The conscious internet users) reveals a significant positive relation with *intention to adopt internet security measures* (*b**= .09, p<.01). Again, although significant, this association is very weak. We can conclude that the PMT model holds true in the context of online security measures and is a valuable theory to base risk communication strategies on.

Table 12: *Regression model where intention to adopt internet security measures is predicted by means of PMT variables, socio-demographic variables and user profile.*

	Intention to adopt internet security measures	
Predictors	Model 1: PMT variables	Model 2: PMT variables, socio-demographic variables and user profile
	b	*b*
Constant	-0,14	-0,11
Perceived severity	0,11**	0,10**
Perceived vulnerability	0,20***	0,21***
Self-efficacy	0,11***	0,11***
Response efficacy	0,09**	0,10**
Attitude	0,16***	0,15***
Subjective norm	0,35***	0,34***
Conscious internet user: yes		0,09**
Male: yes		-0,08**
Adj. R^2	0,33	0,34
F	86,66***	68,81***

N= 1036
* p<.05. ** p<.01. *** p<.001

3.2 Received information and intention to perform security related behavior

In the survey, two information-related items were used. The first one was used to measure to what extent the respondents are informed about risks and the second one to measure to what extent they are informed about how to avoid these risks. If we want a risk communication campaign to be effective, we expect a correlation between the receiving of information and the intention to perform security related behavior. To test this hypothesis a series of Pearson correlations were performed between the two information-related items and the various PMT variables (of which intention is the outcome variable). Following the PMT model, the results show that the receiving of risk-related information has a two-way impact on intention to perform internet security measures.

Indeed, some PMT variables seem to correlate in a negative way with to what extent respondents feel informed about (how to avoid) risks. More specifically, the variable *to what extent respondents feel informed about risks* significantly correlates in a negative way with *perceived vulnerability* (r(1040)= -0,21, p< .01). The variable *to what extent respondents feel informed about how to avoid risks* shows a negative correlation with *perceived vulnerability* (r(1040)= -0,20, p< .01) as well as with *perceived severity* (r(1040)= -0,08, p< .05). Although these correlations are low, they are worth mentioning. Indeed, they indicate that the receiving of risk-related information leads to a lower perceived vulnerability and severity of cybercrime. Following the PMT model, this would mean that risk-related information has a negative impact on *intention to take internet security measures*. Indeed, the variable *to what extent respondents feel informed about how to avoid risks* is negatively correlated with this intention (r(1040)= -0,10, p< .01). The more people are informed about risks on the internet and how to avoid them, the more confident they feel about the safety of the internet (respectively r(1162)= 0,45, p< .01, r(1162)= 0,47, p< .01). Although this may look a positive thing at first sight, we also have to be careful about this as these confident feelings do not necessarily match reality and can potentially minimize existing threats.

On the other hand, the variable to what extent respondents feel informed about risks and how to avoid risks also holds positive correlations with the PMT variables. Both for *self-efficacy* (respectively r(1040)= 0,43, p< .01, r(1040)= 0,46, p< .01) and *response efficacy* (respectively r(1040)= 0,26, p< .01, r(1040)= 0,24, p< .01) a significant positive correlation was found. Moreover, these correlations are relatively strong in comparison with *perceived vulnerability, perceived severity* and *intention*.

As such we can conclude that **risk communication must inform the public, with great care of pointing out the severity of crimes and the vulnerability of users**. This should be done in order to prevent a false feeling of safety. Although correlations do not imply causality, these findings plead in favour of **educating people and sensitizing them about the dangers on the internet** (perceived severity and vulnerability), whilst giving them the **confidence to take measures on their own** (self-efficacy) and **confidence in the effectiveness of security measures** (response efficacy).

When comparing the different user profiles concerning to what extent they are informed about risks and how to avoid them, we notice not much unexpected findings. For both variables, Profile 3 (The inexperienced internet users) differs significantly from Profile 1 (The conscious internet users) and Profile 4 (The resolved internet users) (F (3, 1079)= 7,43, p<.001, F (3, 1079)= 9,79, p<.001). The difference is the strongest for the information about risk avoidance, between the respondents belonging to Profile 3 (The inexperienced internet users) and Profile 4 (The resolved internet users) (*M*= 2,92, *SD*= 1,00 vs. *M*= 3,32, *SD*= 0,95).

3.3 PMT and the four user profiles

Before comparing the mean scores of the four user profiles on the various PMT variables, we will first investigate to what extent the variable *intention to adopt internet security measures* is explained by these variables for the different profiles. Indeed, it has not much value to determine what profile scores highest on, for example, perceived severity when this does not affect to the intention to take internet security measures.

Table 13: *Regression model where intention to adopt internet security measures is predicted by means of PMT variables and socio-demographic variables for* ***Profile 1 - The conscious internet users***

	Intention to adopt internet security measures	
Predictors	Model 1: PMT variables	Model 2: PMT variables, socio-demographic variables
	b	*b*
Constant	0,17	0,25
Perceived vulnerability	0,16**	0,17***
Attitude	0,38***	0,38***
Subjective norm	0,33***	0,33***
Male: yes		-0,09*
Adj. R^2	0,32	0,33
F	53,68***	41,75***

N= 331
* p<.05. ** p<.01. *** p<.001

The *intention to adopt internet security measures* by the respondents belonging to Profile 1 – The conscious internet users, can be predicted by three variables in our PMT model. Somewhat surprising is that the factors *perceived severity*, *self-efficacy* and *response efficacy* do not seem to have any significant predictive power. The model is significant, F (4, 326)= 41,75, p<.001, and has an average predictive power (R^2= 0,33). When controlling for socio-demographic variables, again only gender has a significant association with the outcome variable. Males show a lower intention (*b**= -0,09, p<.01) to adopt security measures than women.

Table 14: *Regression model where intention to adopt internet security measures is predicted by means of PMT variables and socio-demographic variables for* ***Profile 2 - The overly confident internet users***

	Intention to adopt internet security measures	
Predictors	Model 1: PMT variables	Model 2: PMT variables and socio-demographic variables
	b	*b*
Constant	-0,70	-0,13
Perceived vulnerability	0,20**	0,21**
Self-efficacy	0,29***	0,26***
Response efficacy	0,20**	0,23**
Subjective norm	0,43***	0,40***
Low educational level: yes		0,17**
Adj. R^2	0,47	0,49
F	31,44***	27,84***

N= 141
* p<.05. ** p<.01. *** p<.001

The *intention to adopt internet security measures* can be predicted by the respondents belonging to Profile 2 – The overly confident internet users, can be predicted by four variables of the PMT model: *perceived vulnerability, self-efficacy*, *response efficacy* and *subjective norm.* The model is significant, F (5, 135)= 27,84, p<.001, and has a rather strong predictive power (R^2= 0,51). When controlling for socio-demographic variables, only educational level has a significant association with the outcome variable. Surprisingly, people with no/primary education show a stronger intention (*b**= 0,17, p<.01) to adopt security measures than people with a higher education.

Table 15: *Regression model where intention to adopt internet security measures is predicted by means of PMT variables and socio-demographic variables for* ***Profile 3 - The inexperienced internet users***

	Intention to adopt internet security measures
Predictors	PMT variables
	b
Constant	-0,05
Perceived severity	0,15**
Perceived vulnerability	0,19***
Self-efficacy	0,19***
Attitude	0,14*
Subjective norm	0,33***
Adj. R^2	0,33
F	37,21***

N= 366

* p<.05. ** p<.01. *** p<.001

The *intention to adopt internet security measures* by the respondents belonging to Profile 3 – The inexperienced internet users, can be predicted by almost all variables of the PMT model. Only *response efficacy* was not a significant predictor. The model as a whole is significant, F (5, 360)= 37,21, p<.001, and has an average predictive power (R^2= 0,33). Not one of the socio-demographic variables contributed significantly to the model.

__Table 16__: *Regression model where intention to adopt internet security measures is predicted by means of PMT variables and socio-demographic variables for* ***Profile 4 - The resolved internet users***

	Intention to adopt internet security measures
Predictors	PMT variables
	b
Constant	0,63
Perceived vulnerability	0,29***
Subjective norm	0,36***
Response efficacy	0,23**
Adj. R^2	0,29
F	27,74***

N= 201

* p<.05. ** p<.01. *** p<.001

The *intention to adopt internet security measures* can be predicted by the respondents belonging to Profile 4 – The resolved internet users, can be predicted by three variables of the PMT model: *perceived vulnerability*, *subjective norm* and *response efficacy*. The model is significant, F (3, 197)= 27,74, p<.001, and has a low predictive power (R^2= 0,29). Not one of the socio-demographic variables contributed significantly to the model.

When we compare the different user profiles with the different PMT variables, we see a rather inconsistent image. Though, as expected, the respondents belonging to Profile 2 (The overly confident internet users) (*M*= 4,14, *SD*= 0,70) perceive cybercrime significantly less severe than the other profiles (F (3, 1036)= 9,14, p<.001).

Concerning self-efficacy, the respondents belonging to Profile 3 (The inexperienced internet users) differ significantly from the respondents belonging to Profile 1 (The conscious internet users) (*M* = 3,17, *SD* = 0,72 vs. *M* = 3,50, *SD* = 0,66, F (3, 1036)= 21,91, p<.001) and Profile 4 (The resolved internet users) (*M* = 3,61, *SD* = 0,66), while the respondents belonging to Profile 4 (The resolved internet users) also differ significantly from the respondents belonging to Profile 2 (The overly confident internet users) (*M* = 3,36, *SD* = 0,70). Hence, the respondents belonging to Profile 1 (The conscious users) and especially Profile 4 (The resolved internet users) have high trust in their ability to take security measures.

As for response efficacy, only the respondents belonging to Profile 3 (The inexperienced internet users) and Profile 4 (The resolved internet users) differ significantly. The latter group believes significantly more than the respondents belonging to Profile 3 (The inexperienced internet users) that the recommended response to avert cyber threats will work (*M* = 3,57, *SD* = 0,62 vs *M* = 3,78, *SD* = 0,64, F (3, 1036)= 5,03, p<.01). This is in line with our previous findings, as we found that the respondents belonging to Profile 4 (The resolved internet users) have great confidence in the protective power of paid software to secure his/her internet use.

As these variables result in a certain attitude and subsequently, intention, one would expect to see similar results with regard to the intention to perform security related behavior. As so, we find that respondents belonging to Profile 1 (The conscious internet users) differ significantly from the respondents belonging to Profile 2 (The overly confident internet users) (*M* = 3,59, *SD* = 0,65 vs *M* = 3,37, *SD* = 0,68, F (3, 1036)= 6,45, p<.001) and Profile 3 (The inexperienced internet users) (*M* = 3,39, *SD* = 0,65).

Also as expected, no significant differences between groups were found for subjective norm and perceived vulnerability, since these two variables are found in all regressions.

3.4 Conclusion

The PMT model proves to be a reliable model in predicting the intention to take internet security measures. Given the fact that the receiving of information about (how to avoid) risks also correlates with the intention to take internet security measures, it is correct to state that the PMT model serves as a trustful model to base risk communication campaigns on.

The respondents belonging to Profile 3 - The inexperienced internet users and Profile 2 - The overly confident internet users, can be considered the two most vulnerable user profiles when it comes to cybercrime. On the one hand they have little knowledge about the threats that exist in an online environment, how serious these are and what they can do to counter them. As such, it should be no surprise that these user profiles are the least informed about internet risks and how to avoid them. Although correlations do not indicate causality, this seems to result in a rather low perceived severity, self-efficacy, response-efficacy and consequently intention to take protective measures.

Another argument to treat these user profiles with priority in risk communication strategies is the fact that no high correlations were found between internet activity, victimization and protective behavior. This makes that the rather inactive and inexperienced internet users (Profile 3) and, to a lesser extent, confident internet users (Profile 2) are exposed to an equal amount of risk as the more active profiles.

As a side note, we want to stress that it is important to keep in mind that all significant correlations and predictors for the different user profiles were rather low. Also, it seems hard to find an explanation why some of the predictors where significant and others not. Only subjective norm and perceived vulnerability were found to be significant predictors for all of the user profiles.

4 Recommendations for risk communication

In the last section of this report, we will make some recommendations that can serve as an input for an efficient and effective risk communication campaign, based on the most relevant findings of the survey. First, we identify the most important target groups to whom risk communication campaigns must be targeted. Second, we provide with some more specific recommendations, pertaining to specific topics and content for risk communication campaigns.

4.1 Target groups

In general we notice that older, less educated people who are residing in Brussels and Wallonia seem to be the most vulnerable citizens when it comes to cybercrime threats. They take less security measures, in comparison to other groups of respondents, and are thus a relatively easy target for cyber-attacks. Consequently, residents from Wallonia and Brussels also suffer the largest financial losses due to cybercrime.

When we take a look at the user typology that we have developed in the course of this analysis, we can conclude that the respondents belonging to Profile 2 (The overly confident internet users) and Profile 3 (The inexperienced internet users) consist mainly out of these older and less educated individuals. Overall, they have little knowledge about internet threats and are the least informed about internet risks and how to avoid them. Hence, they are identified as our most important target groups. Communication and awareness campaigns should especially take into account the specificities of these internet user profiles.

4.2 Topics and content

Although the respondents belonging to Profile 3 (The inexperienced internet users) and Profile 2 (The overly confident internet users) share a common socio-demographic profile (i.e. the majority of them tend to be older), there is a difference in their risk perception and thus they should be approached with a different risk communication approach. What content or message a risk communication campaign must carry depends on which angle of incidence is being used. One or more of the different PMT variables can be emphasized, but as we have argued, a one-sided message can be dangerous. Risk communication must sensitize the citizen about the potential dangers that exist on the internet (perceived severity and vulnerability), whilst giving them the confidence to take measures on their own (self-efficacy) and confidence in the effectiveness of security measures (response efficacy). This balance is very delicate, since too little emphasis on perceived severity and vulnerability could result in a false feeling of "informed confidence". On the other hand, too much emphasis on these aspects could cause maladaptive coping behavior. Especially with regard to the more vulnerable and inexperienced users (Profile 3) this seems to be important. Risk campaigns directed at this user profile must carry a message that stimulates perseverance in the online environment.

This said, there are multiple specific topics that arose out of the survey and can be used as content to anticipate on the variables in the PMT model. One possible risk communication effort could be concentrated on certain types of risky internet behavior. Indeed, the survey pointed out that downloading and buying/selling goods or services are activities that are vulnerable to respectively viruses and scams. The police virus/ransomware seemed to make the most victims. In an ideal PMT-driven risk communication model, people are sensitized and informed about these dangers and given information about how to deal with them. In this regard, it is important to point at the various kinds of security measures that exist. Indeed, the survey shows that too much people (the respondents belonging to Profile 1 - The conscious internet users, to a lesser extent) rely on just one security measure. The existence and importance of the various sorts of security measures must be made clearer.

Another point of incidence to stimulate security related behavior could be to point out the cost, direct or indirect, which is caused by cybercrime. This could be a convincing argument, especially since the survey shows that scams, hacking and viruses are often accompanied with considerable financial losses. Consequently, they are perceived as more severe, and are often more reported. Stressing these financial risks could be an effective way to stimulate people in taking security measures.

To conclude we discuss three communication efforts that do not involve risk perception or the stimulation of security-related behavior. First of all, a note can be made about governmental and corporate surveillance. Although this this of cybercrime is not necessarily dangerous or even illegal (though often dubious), it is important that individuals are aware that this happens, so they can act like informed and conscious users. The survey pointed out that especially older and less educated individuals are not aware of corporate surveillance and the commodification of personal data in a commercial context.

The data also revealed that younger people are significantly more confronted with unwanted content/behavior. Again, this is not so much a matter of what protective measurements to take, but learning individuals how to use the internet in a responsible way and how to deal with inappropriate content and behavior seems to be important here. More specifically, security campaigns or other public interventions can concentrate on the risks of careless sharing, online bullying and sexual harassment.

A final communication effort could focus on the reporting of victimization. Indeed, little victims report cybercrime, especially when there was no or negligible financial loss. Though, this is important to form a consistent, realistic and informed image of cybercrime in Belgium.

4.3 Conclusion

As an input for setting up information and user awareness campaigns, it is important to take into account the preferred target population as well as the content. Based on the typology of internet users, two groups (respondents belonging to Profile 2 and Profile 3) deserve particular attention. When it comes to the content of campaigns, we propose that a balance needs to be found between on the one hand informing citizens about the potential dangers of the internet, while on the other hand giving them confidence to take measures on their own behalf and inform them about the effectiveness of taking internet security measures.

DISCUSSION

Although the PMT model is a valuable contribution to this study and has provided some useful insights, it is necessary to put some of these findings in perspective. Indeed, end-users perform security behavior in the context of their daily lives, as a sociable accountable and resource-limited activity. Hence, awareness of cybercrime and resulting security actions are dependent on (1) users' concrete experiences of cybercrime (and accompanying losses, if applicable); and (2) are socially organized and bound to users' broader activities (Rughiniş and Rughiniş, 2014).

With this first remark we point to the fact that awareness of cybercrime has an important influence on the conscious experience of cybercrime, and thus the reporting in the survey. When respondents have no knowledge about cybercrime or its specific vocabulary, they may not recognise it. Also, the experience of loss influences the reporting in this survey. End-users are often protected from cybercrime risks by arrangements that transfer financial losses to corporate actors. Losses may also be hidden, in the form of minor inconveniences or opportunity costs (Rughiniş and Rughiniş, 2014). Secondly, awareness of cybercrime is socially organized. This means that security measures are not justifiable per se. Users need to account for their actions in their social groups, as reasonable responses to recognized risks. In this regard it also important that these decisions are recognized as competent decisions of their own, rather than obeying external directives or acting out of fear (Rughiniş and Rughiniş, 2014). This is something to think about when designing communication strategies. It must be said that the PMT model partly anticipates on this notion by the integration of the concept of "subjective norm", though this might not be sufficient to capture everything. In the same perspective, loss and responsibility are also socially organised. Indeed, users may not always be held responsible for security failures. Risks only appear as relevant through social activity, in which events happen, are interpreted and blame and merit is assigned (Rughiniş and Rughiniş, 2014).

In addition, users differ in their security-related intention/behavior, depending on the social organization of their activity, the frequency and intensity of exposure to personal losses, available justifications for their security behavior to significant others and on the resources of technical expertise they have (Rughiniş and Rughiniş, 2014). This should be taken into account when studying cybercrime awareness.

Also the role of the body, institution or organisation that carries out the risk communication campaign must be taken into account when preparing and evaluating the effectiveness of a campaign. Indeed, according to the "Trust and Confidence model", trust in institutions (in this case the government) is an important factor in the public's judgments of risks and benefits, and consequently their acceptance of recommended measures (Weerd, Timmermans, Beaujean, Oudhoff & Steenbergen, 2011; Siegrist, Earle, Gutscher, 2003). In this respect, it is reassuring that Belgians seem to have quite some confidence in their government and parliament. While 43% of the Belgian population tends to trust the government, 44% tends to trust the parliament. This ranks Belgium respectively on the ninth and seventh place of EU countries (Eurobarometer, 2014).

.

CONCLUSION

We still have a long road ahead when it comes to raising awareness about the different threats that one can encounter in the online world. Indeed, quite a large number of people associate cybercrime with viruses and hacking, without further thinking about the purposes or consequences of the malware or intrusion.

Based on the survey data we were able to construct a typology of four distinct internet user profiles using a cluster analysis: These profiles were labelled 'The conscious internet users' (Profile 1), 'The overly confident internet users' (Profile 2), 'The inexperienced internet users' (Profile 3) and 'The resolved internet users' (Profile 4). This segmentation was based on four factors, being frequency and variety of internet use, the variety of security measures the respondents take and how safe they perceive certain internet activities. Especially the respondents belonging to Profile 3 (The inexperienced internet users) and Profile 2 (The overly confident internet users) turned out to be quite vulnerable for cybercrime threats in the online context. They are most often less educated, elder individuals and uninformed about the risks of the internet. As for the inexperienced internet users (Profile 3) this results in prudent, maladaptive coping behavior like reducing internet use, while the overly confident internet users (Profile 2) mainly ignore and minimalizes these risks. Anyhow, they are little protected against the various types of cybercrimes.

Considering cybercrime victimization, it is possible to sum up a number of important findings, allowing for a better insight into this phenomenon in Belgium. First of all, viruses seem to be the biggest threat in terms of occurrence, followed by corporate surveillance and surveillance by the government. At the same time, however, it also interesting to find out that quite a large number of people do not know exactly how many viruses they became victim of, endorsing the fact that there appears some fuzziness around the phenomenon. Also, scams and hacking occur much less, while these types of cybercrime cause much bigger costs. Hence, they are perceived as the most severe types of cybercrime and are consequently more reported in comparison to the other types of cybercrime. Especially downloading and buying/selling goods or services seem to be risky internet activities, since these are the main sources from which scams and viruses arise. When people are confronted with unwanted content or behavior online, this is mainly sexual content or spam.

Over all, people who are less educated seem to be victimized the most. Our results also see residence as an important factor, as people who are residing in Wallonia seem to be more often the victim of cybercrime. At the same time, however, it are mainly the conscious internet users (Profile 1) that indicate to encounter the most cybercrimes. This finding can be explained by the fact that the inexperienced internet users (Profile 3) and the overly confident internet users (Profile 2) do not recognize these cybercrimes as such. Indeed, younger and more IT-literate respondents (from which the conscious internet users mainly consist) indicate to encounter more cybercrimes.

The PMT model proves to be a reliable model in predicting the intention to take internet security measures. Given the fact that the receiving of information about (how to avoid) risks also correlates with intention to take internet security measures, we can state that the PMT model serves as a trustful model to base risk communication campaigns on. For our two most vulnerable profiles (Profile 3 – the inexperienced internet users, and Profile 2 – the overly confident internet users), this means that they have a rather low perceived severity, self-efficacy, response-efficacy and consequently intention to take protective measures. At the same time, it is important to keep in mind that all significant correlations and predictors for the different user profiles were rather low. In addition, it seems hard to find an explanation why some of the predictors where significant and others not. Only subjective norm and perceived vulnerability were found to be significant predictors for all of the user profiles.

Considering concrete suggestions for risk communication campaigns, this research suggests to first of all concentrate on citizens that match the profiles of the overly confident internet users (Profile 2) and the inexperienced internet users (Profile 3). It is especially important to maintain a well-considered balance between sensitizing citizens about the risks that exist on the internet (perceived severity and vulnerability), whilst giving them the confidence to take measures on their own (self-efficacy) and confidence in the effectiveness of security measures (response efficacy). Especially with regard to the more vulnerable and inexperienced users, this seems to be an important strategy. Risk communication campaigns that are targeted towards this user profile must carry a message that stimulates perseverance in the online environment. More specifically, risk communication can focus on the different kinds of internet activities that are vulnerable to viruses and scams, point to the different kinds of security measures that exist, and make clear that one measure is often not enough to protect against all threats. Another point of incidence could be to point out the cost that is caused by cybercrime, be it direct or indirect costs. Especially scams, hacking and viruses are often accompanied with considerable financial losses. Furthermore, it is possible to raise awareness about the commodification of data (via corporate surveillance), concentrating on the risks of careless sharing, online bullying and sexual harassment, or focus on a higher report rate of cybercrime.

FUTURE RESEARCH

Although the value of this research is undeniable, there are some limitations as well. One limitation is that there was most probably an underestimation of victimization. Respondents may interpret different events in their online life as security breaches or not, and they may not even notice them, if they are not familiar with a specific vocabulary that labels and explains such events (Böhme & Moore, 2012).

Another limitation results from the way that "victimization" was inquired, particularly in the survey questions. Indeed, this was often interpreted as an "attempt to", as could be deviated from the open questions. A better solution here would have been to explicitly state that there needs to be a certain kind of cost (financial, psychological, physical, etc.) before one could treat himself as a "victim". Future research could benefit from a better conceptualization and operationalization of cybercrime.

With regard to the results in relation to the PMT model, it is necessary to keep in mind that users differ in their security-related intention/behavior, depending on the social organization of their activity, the frequency and intensity of exposure to personal loss(es), available justifications for their security behavior to significant others and on the resources of technical expertise they have. Indeed, it is not possible to "reduce" *intention to take internet security measures* into six predictors, nor is it possible to deduct simple causal relations (given the negative feedback loop). Nevertheless, we believe that this model is still a valuable base for the construction of risk communication campaigns, as long as this is complemented with other research methods like classification analysis. Future research should also take this into account.

REFERENCES

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimethod empirical examination of home computer users security behavioral intentions. *MIS Quarterly, 34(3)*, 613-643.

Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the cost of cybercrime. In: *The Economics of Information Security and Privacy* (pp. 265-300). Springer Berlin Heidelberg.

Böhme, R., & Moore, T. (2012). Challenges in empirical security research. Retrieved on the 13th of April, 2015, from http://lyle.smu.edu/~tylerm/courses/econsec/reading/lnse-survey.pdf.

Cert.be – The Federal Cyber Emergency Team (2015). *Press release: Number of cyber incidents doubled in 2014*. Consulted on the 11th of March, 2015, from https://www.cert.be/docs/press-release-number-cyber-incidents-doubled-2014.

Crossler, R., & Bélanger, F. (2014). An extended perspective on individual security behaviors: Protection Motivation Theory and a Unified Security Practices (USP) instrument. *ACM SIGMIS Database, 45(4),* 51-71.

Datanews.knack.be (2015). "*Twee keer meer cyberincidenten in ons land*". Consulted on the 11th of March, 2015, from http://datanews.knack.be/ict/nieuws/twee-keer-meer-cyberincidenten-in-ons-land/article-normal-540345.html

DeMorgen.be (2015). *"Er dreigt een grote internetcrash"*. Consulted on the 13th of April, 2015, from http://www.demorgen.be/technologie/-er-dreigt-een-grote-internetcrash-a2285314/

Deredactie.be (2015). *"Belgisch leger krijgt cybercomponent naast traditionele land-, lucht- en zeemacht".* Consulted on the 7th of April, 2015, from http://deredactie.be/cm/vrtnieuws/politiek/1.2296591

De Jonge, J., van Trijp, H., Renes, R. J., & Frewer, L. (2007). Understanding consumer confidence in the safety of food: Its two-dimensional structure and determinants. *Risk Analysis, 27(3),* 729-740.

De Tijd (2015). *"GSM miljoenen Belgen kan worden afgeluisterd".* Consulted on the 21th of February, 2015.

Digimeter (2014). Measuring digital media trends in Flanders (iMinds). Request of report possible on https://www.iminds.be/en/gain-insights/digimeter

Eurobarometer (2013). Special Eurobarometer 404 / Wave EB79.4: Cyber security report. TNS Opinions & Social. Consulted from http://ec.europa.eu/public_opinion/index_en.htm

Eurobarometer (2014). http://ec.europa.eu/public_opinion/archives/eb/eb81/eb81_first_en.pdf. Consulted from http://ec.europa.eu/public_opinion/index_en.htm

FPS Economy (FOD Economie) – Barometer van de informatiemaatschappij (2015). Published 16/07/2015 on:

http://economie.fgov.be/nl/modules/publications/statistiques/arbeidsmarkt_levensomstandigheden/barometer_van_de_informatiemaatschappij_2015.jsp

FPS Economy (FOD Economie) – Statistics and figures (2014). 2014 age, residence and gender statistics of Belgian citizens. Consulted from http://economie.fgov.be/nl/statistieken/cijfers/bevolking/structuur/

Greenfield, V.A., & Paoli, L. (2013). A framework to assess the harms of crimes. *British Journal of Criminology, 53(5),* 864-885.

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

Internetlivestats.com (2015). Part of the Real Time Statistics Project (Worldometers and 7 Billion World). Consulted on the 4th of May, from https://www.internetlivestats.com

Marakas, G. M., Johnson, R. D., & Clay, P. F. (2007). The evolving nature of the computer self-efficacy construct: An empirical investigation of measurement construction, validity, reliability and stability over time. *Journal of the Association for Information Systems, 8(1),* 2.

Riek, M., Böhme, R., & Moore, T. (2014). Understanding the influence of cybercrime risk on the e-service adoption of European internet users. In *Proceedings of the 13th Workshop on the Economics of Information Security (WEIS)*, The Pennsylvania State University, State College, Pennsylvania (working paper).

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *Journal of Psychology, 91(1)*, 93-114.

Rughiniş, & Rughiniş (2014). Nothing ventured, nothing gained. Profiles of online activity, cyber-crime exposure, and security measures of end-users in European Union. *Computers & Security, 43*, 111-125.

Siegrist, M., Earle, T.C., Gutscher, H. (2003). Test of a trust and confidence model in the applied context of Electromagnetic Field Risks (EMF), *Risk Analysis*, *23*, 705-716.

Singer, P. W., & Friedman, A. (2014). The 5 biggest cybersecurity myths, debunked. Published on Wired.com on 04/02/2014.

Staysafeonline.org (2015). Powered by the National Cyber Security Alliance. Consulted on the 12th of March, 2015, from https://www.staysafeonline.org/stay-safe-online/resources/

Veiligheidsmonitor (2013). Consulted from http://www.veiligheidsmonitor.nl, and 'Centraal Bureau voor de Statistiek (CBS)' http://www.cbs.nl

Van der Weerd, W., Timmermans, D., Beaujean, D., Oudhoff, J., Steenbergen, J.E. (2011). Monitoring the level of government trust, risk perception and intention of the general public to adopt protective measures during the influenza A (H1N1) pandemic in the Netherlands, *BMC Public Health, 11*(575), 1-12.

Witte, K. (1996). Predicting risk behaviors: Development and validation of a diagnostic scale. *Journal of Health Communication, 1(4),* 317-342.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education & Behavior, 27(5)*, 591-615.

APPENDIX – SURVEY AS LAUNCHED

Vous pouvez modifier la langue dans le coin supérieur de chaque page.
You can change the language in the upper right corner of each page.
U kunt de taal wijzigen in de rechterbovenhoek van elke pagina.

Dear Sir/Madam,

First of all, we would like to thank you for your willingness to take part in this study on **internet safety**.

Please read, and complete, all the questions carefully. The data obtained from this study are **anonymous**, **strictly confidential** and not passed on to third parties.

Thank you for your cooperation,

The research team of iMinds-MICT-UGent

Q1 Which **equipment** do you have at your disposal **at home**?
(multiple answers possible)

□ Desktop computer
□ Laptop
□ Tablet (e.g. iPad)
□ Smartphone (e.g. Samsung Galaxy)
□ Gaming console (e.g. PlayStation 4)
□ Other: ___
□ None of the above

Q3 How often do you use the **internet** during a typical week?
You can answer by clicking on the balls.

	Never	Less than weekly	Less than daily	Less than 1 hour per day	Between 1 and 3 hours per day	More than 3 hours per day
At home during work days	○	○	○	○	○	○
At home during the weekend	○	○	○	○	○	○
At work	○	○	○	○	○	○

Q4 Which of the following **activities** have you done in the **past month** using your device(s)?
Tip: work your way down (activities) and from left to right (devices).

	Desktop computer	Laptop	Tablet	Smartphone	Gaming console	Other (Q1)
Information retrieval	□	□	□	□	□	□
News sites	□	□	□	□	□	□
E-mail	□	□	□	□	□	□
Electronic banking	□	□	□	□	□	□
Online gaming (incl. games on Facebook or other websites)	□	□	□	□	□	□
Social media (e.g. Facebook, Twitter)	□	□	□	□	□	□
Chatting	□	□	□	□	□	□
Phone calls over the internet (e.g. Skype, FaceTime)	□	□	□	□	□	□
Purchase and/or sell goods (e.g. music, films, software, books, clothes)	□	□	□	□	□	□
Download (e.g. music, films, software, books)	□	□	□	□	□	□
Streaming (playing files via internet, without downloading them first, e.g. YouTube)	□	□	□	□	□	□

Q5 To what extent do you **agree** with the following statements?

	Totally disagree	Disagree	Neutral	Agree	Totally agree
I am optimistic about the safety of the internet.	○	○	○	○	○
I feel adequately informed about the risks of the internet.	○	○	○	○	○
I am concerned about internet safety.	○	○	○	○	○
I have every confidence that the internet is safe.	○	○	○	○	○
I am satisfied with the safety of the internet.	○	○	○	○	○
I feel adequately informed about how to avoid the risks of the internet.	○	○	○	○	○

Q6 How **safe** do you think these activities are in general?

	Not safe at all	Not safe	Neutral	Safe	Very safe	I don't know (it)
Information retrieval	○	○	○	○	○	○
News sites	○	○	○	○	○	○
E-mail	○	○	○	○	○	○
Electronic banking	○	○	○	○	○	○
Online gaming (incl. games on Facebook or other websites)	○	○	○	○	○	○
Social media (e.g. Facebook, Twitter)	○	○	○	○	○	○
Chatting	○	○	○	○	○	○
Phone calls over the internet (e.g. Skype, FaceTime)	○	○	○	○	○	○
Purchase and/or sell goods (e.g. music, films, software, books, clothes)	○	○	○	○	○	○
Download (e.g. music, films, software, books)	○	○	○	○	○	○
Streaming (playing files via internet, without downloading them first, e.g. YouTube)	○	○	○	○	○	○

Q7 In your opinion, how **serious** are the following phenomena?

	Not serious at all	Not serious	Neutral	Serious	Very serious
Viruses (e.g. malware, botnets)	○	○	○	○	○
Scams (e.g. in online banking)	○	○	○	○	○
Piracy (downloading illegally)	○	○	○	○	○
Hacking (e.g. unlawful access, identity theft)	○	○	○	○	○
Monitoring by government (collecting data about you)	○	○	○	○	○
Monitoring by companies (collecting data about you)	○	○	○	○	○
Unwanted content and/or behavior (e.g. sexual or racist content, cyberbullying, stalking)	○	○	○	○	○

Q8 How **likely** is it that you will become a victim of the following phenomena?

	Very unlikely	Unlikely	Neutral	Likely	Very likely
Viruses (e.g. malware, botnets)	○	○	○	○	○
Scams (e.g. in online banking)	○	○	○	○	○
Hacking (e.g. unlawful access, identity theft)	○	○	○	○	○
Monitoring by government (collecting data about you)	○	○	○	○	○
Monitoring by companies (collecting data about you)	○	○	○	○	○
Unwanted content and/or behavior (e.g. sexual or racist content, cyberbullying, stalking)	○	○	○	○	○

Q9 Have **you**, or anyone else in your **family**, experienced any of the following situations in the **past 12 months**?

	Yes, myself	Yes, someone else in my family	Yes, both me and someone else in my family (e.g. shared computer)	I suppose so	No	I don't know
Viruses (e.g. malware, botnets)	○	○	○	○	○	○
Scams (e.g. in online banking)	○	○	○	○	○	○
Hacking (e.g. unlawful access, identity theft)	○	○	○	○	○	○
Monitoring by government (collecting data about you)	○	○	○	○	○	○
Monitoring by companies (collecting data about you)	○	○	○	○	○	○
Unwanted content and/or behavior (e.g. sexual or racist content, cyberbullying, stalking)	○	○	○	○	○	○

Q10 Do you believe these incidents had **financial consequences?**
Think of the cost of the incurred damage, protective measures and/or repairing.

	€ 0	Less than € 20	Less than € 200	Less than € 2,000	€ 2,000 or more	I don’t know
Viruses (e.g. malware, botnets)	❍	❍	❍	❍	❍	❍
Scams (e.g. in online banking)	❍	❍	❍	❍	❍	❍
Hacking (e.g. unlawful access, identity theft)	❍	❍	❍	❍	❍	❍
Monitoring by government (collecting data about you)	❍	❍	❍	❍	❍	❍
Monitoring by companies (collecting data about you)	❍	❍	❍	❍	❍	❍
Unwanted content and/or behavior (e.g. sexual or racist content, cyberbullying, stalking)	❍	❍	❍	❍	❍	❍

Q11 Viruses
(e.g. malware, botnets)

In the **past 12 months**, how often have you and/or other members of your family been a victim of **viruses**?

❍ Once
❍ Twice
❍ Three times
❍ Four times
❍ Five or more times
❍ I don't know

Q12 Viruses
(e.g. malware, botnets)

This question is about the last time you(r family) were/was a victim.

What exactly was damaged or infected?
(multiple answers possible)

- □ Hardware (e.g. the device itself)
- □ Software (e.g. programs or apps)
- □ File(s) (e.g. documents or photos)
- □ Network(s) (e.g. LAN or intranet)
- □ Website(s)
- □ Account(s)
- □ Other: ____
- □ I don't know

Q13 Viruses
(e.g. malware, botnets)

These questions are about the last time you(r family) were/was a victim.

Can you **describe** the incident briefly?

____

Q14 Was this incident **reported**?
(multiple answers possible)

- □ Yes, with the police
- □ Yes, with the internet provider
- □ Yes, with another body: ___
- □ No

Q15 Scams

(e.g. in online banking)

In the **past 12 months**, how often have you and/or other members of your family been a victim of **scams**?

○ Once
○ Twice
○ Three times
○ Four times
○ Five or more times
○ I don't know

Q16 Scams

(e.g. in online banking)

This question is about the last time you(r family) were/was a victim.

When did the scam and/or theft take place?
(multiple answers possible)

□ When banking online
□ When buying goods/services
□ When selling goods/services
□ On another occasion: ___
□ I don't know

Q17 Scams

(e.g. in online banking)

These questions are about the last time you(r family) were/was a victim.

Can you **describe** the incident briefly?

____

Q18 Was this incident **reported**?
(multiple answers possible)

□ Yes, with the police
□ Yes, at the bank/financial institution
□ Yes, at a consumer organisation
□ Yes, with another body: ___
□ No

Q19 Hacking
(e.g. unlawful access, identity theft)

In the **past 12 months**, how often have you and/or other members of your family been a victim of **hacking**?

○ Once
○ Twice
○ Three times
○ Four times
○ Five or more times
○ I don’t know

Q20 Hacking
(e.g. unlawful access, identity theft)

This question is about the last time you(r family) were/was a victim.

What exactly happened?
(multiple answers possible)

□ A device was broken into/unlawfully logged into.
□ A network was broken into/unlawfully logged into.
□ An e-mail account was broken into/unlawfully logged into.
□ A website was broken into/unlawfully logged into.
□ A social media account was broken into/unlawfully logged into.
□ Something else: ___
□ I don't know

Q21 Hacking
(e.g. unlawful access, identity theft)

These questions are about the last time you(r family) were/was a victim.

Can you **describe** the incident briefly?

____

Q22 Was this incident **reported**?
(multiple answers possible)

□ Yes, with the police
□ Yes, with the internet provider
□ Yes, at the company behind the social media or website (e.g. Facebook, Twitter)
□ Yes, with another body: ___
□ No

Q23 Monitoring by government
(collecting data about you)

In the **past 12 months**, how often have you and/or other members of your family experienced **monitoring by the government**?

○ Once
○ Twice
○ Three times
○ Four times
○ Five or more times
○ I don't know

Q24 Monitoring by government
(collecting data about you)

This question is about the last time you(r family) experienced this.

What exactly happened?
(multiple answers possible)

□ My data were used without my knowledge.
□ My data were used without my explicit permission.
□ Something else: ___
□ I don't know

Q25 Monitoring by government
(collecting data about you)

These questions are about the last time you(r family) experienced this.

If possible, can you **describe** the incident briefly?

____

Q26 Was this incident **reported**?
(multiple answers possible)

□ Yes, with the police
□ Yes, with the government agency in question
□ Yes, with the internet provider
□ Yes, with another body: ___
□ No

Q27 Monitoring by companies
(collecting data about you)

In the **past 12 months**, how often have you and/or other members of your family experienced **monitoring by companies**?

○ Once
○ Twice
○ Three times
○ Four times
○ Five or more times
○ I don't know

Q28 Monitoring by companies
(collecting data about you)

This question is about the last time you(r family) experienced this.

What exactly happened?
(multiple answers possible)

□ My data were used without my knowledge.
□ My data were used without my explicit permission.
□ Something else: ___
□ I don't know

Q29 Monitoring by companies
(collecting data about you)

These questions are about the last time you(r family) experienced this.

If possible, can you **describe** the incident briefly?

____

Q30 Was this incident **reported**?
(multiple answers possible)

❑ Yes, with the police
❑ Yes, with the private company in question
❑ Yes, with the internet provider
❑ Yes, with another body: ___
❑ No

Q31 Unwanted content and/or behavior
(e.g. sexual or racist content, cyberbullying, stalking)

In the **past 12 months**, how often have you and/or other members of your family been a victim of **unwanted content and/or behavior**?

○ Once
○ Twice
○ Three times
○ Four times
○ Five or more times
○ Don't know

Q32 Unwanted content and/or behavior
(e.g. sexual or racist content, cyberbullying, stalking)

This question is about the last time you(r family) were/was a victim.

What exactly did you get in touch with?
(multiple answers possible)

❑ Inappropriate content of a sexual nature
❑ Inappropriate content of a racist and/or discriminating nature
❑ Inappropriate content inciting violence, terrorism and/or extremism
❑ Inappropriate sexual behavior
❑ Inappropriate behavior: stalking
❑ Inappropriate behavior: bullying
❑ Inappropriate behavior: swearing and/or threatening
❑ Something else: ___
❑ I don't know

Q33 Unwanted content and/or behavior
(e.g. sexual or racist content, cyberbullying, stalking)

These questions are about the last time you(r family) were/was a victim.

Can you **describe** the incident briefly?

____

Q34 Was this incident **reported**?
(multiple answers possible)

- □ Yes, with the police
- □ Yes, to the website administrator/moderator
- □ Yes, at the company behind the social media or website (e.g. Facebook, Twitter)
- □ Yes, with the internet provider
- □ Yes, with another body: ___
- □ No

Q35 Do you take one or more of the following **security measures** to protect yourself or your family against such incidents?
(multiple answers possible)

Tip: work your way down (incidents) and from left to right (safety measures).

	Reduce internet use (e.g. download less, use social media less)	Avoid or stop certain activities (e.g. ignore certain mails, refrain from online banking)	Change settings (e.g. privacy settings on social media, spam filter, change passwords)	Creating a backup	Install software (paying)	Install software (non-paying)
Viruses (e.g. malware, botnets)	○	○	○	○	○	○
Scams (e.g. in online banking)	○	○	○	○	○	○
Hacking (e.g. unlawful access, identity theft)	○	○	○	○	○	○
Monitoring by government (collecting data about you)	○	○	○	○	○	○
Monitoring by companies (collecting data about you)	○	○	○	○	○	○
Unwanted content and/or behavior (e.g. sexual or racist content, cyberbullying, stalking)	○	○	○	○	○	○

Q36 To what extent do you **agree** with the following statements?

To keep statements brief, **« cybercrime »** is used as a blanket term for internet-related risks.

Security measures are measures you, as an internet user, can take to protect yourself against internet-related risks.
Examples: anti-virus software, change privacy settings, software that blocks pop-up windows.

	Totally disagree	Disagree	Neutral	Agree	Totally agree
It is possible that I will be a victim of cybercrime.	❍	❍	❍	❍	❍
Taking security measures is a good idea.	❍	❍	❍	❍	❍
I believe that cybercrime is significant.	❍	❍	❍	❍	❍
Taking the necessary security measures is entirely under my control.	❍	❍	❍	❍	❍
I am likely to take (more) security measures.	❍	❍	❍	❍	❍
Security measures are effective in preventing cybercrime.	❍	❍	❍	❍	❍
I like the idea of taking security measures.	❍	❍	❍	❍	❍
People to whom I look up to find that I should protect myself against cybercrime.	❍	❍	❍	❍	❍
I am certain that I will take (more) security measures.	❍	❍	❍	❍	❍
Please respond with « Totally agree » for this item/question.	❍	❍	❍	❍	❍
Taking the necessary security measures is easy.	❍	❍	❍	❍	❍
My friends think that I should protect myself against cybercrime.	❍	❍	❍	❍	❍
I don't have the knowledge and skills to take the necessary security measures.	❍	❍	❍	❍	❍

Q37 To what extent do you **agree** with the following statements?

To keep statements brief, **« cybercrime »** is used as a blanket term for internet-related risks.

Security measures are measures you, as an internet user, can take to protect yourself against internet-related risks.
Examples: anti-virus software, change privacy settings, software that blocks pop-up windows.

	Totally disagree	Disagree	Neutral	Agree	Totally agree
I believe that cybercrime is serious.	○	○	○	○	○
It is likely that I will be a victim of cybercrime.	○	○	○	○	○
By taking protective measures, I can prevent cybercrime.	○	○	○	○	○
Taking security measures is important.	○	○	○	○	○
I feel comfortable taking security measures.	○	○	○	○	○
It is possible that I will take (more) security measures.	○	○	○	○	○
I have the knowledge and skills to take the necessary security measures.	○	○	○	○	○
People with whom I compare myself, find that I should protect myself against cybercrime.	○	○	○	○	○
I believe that cybercrime is severe.	○	○	○	○	○
If I take security measures, I am less likely to be a victim of cybercrime.	○	○	○	○	○
There is a great risk that I'll be a victim of cybercrime.	○	○	○	○	○

Q38 What is your **gender**?

○ Male
○ Female

Q39 What **year** were you born?

○ Born after 1997
○ 1997
○ 1996
○ …
○ 1915

Q40 Where do you **live**?

❍ Flanders
❍ Wallonia
❍ Brussels

Q41 What is your **profession**?

❍ Student
❍ Worker
❍ Clerk
❍ Management/executive
❍ Self-employed/professional
❍ Civil servant
❍ Housewife/househusband
❍ Jobseeker
❍ (Semi-)retired
❍ Incapacitated for work/on long-term sick leave
❍ Other, namely: ___

Q42 What is your highest **diploma**?

❍ No diploma
❍ Primary
❍ Lower secondary
❍ Upper secondary (ASO)
❍ Upper secondary technical or art (TSO/KSO)
❍ Upper secondary vocational (BSO)
❍ Higher non-university/Bachelor
❍ (Post-)graduate/Master

Q43 What best describes your **family situation**?

Minors are children under 18.

○ Married/living together without minor children
○ Married/living together with minor child(ren)
○ Single without minor children
○ Single with minor child(ren)
○ Living with parent(s)/relatives
○ Living with others
○ Student in student accommodation/digs