Onderzoeksgroep voor Media, Innovatie en
CommunicatieTechnologieën
Universiteit Gent
Campus Aula
Korte Meer 7-9-11, 9000 Gent
09/264 97 07
http://www.mict.be

Measuring the cost and impact of cybercrime in Belgium (BCC): D3.1.2 Risk perception monitor report (2nd wave, 2017)

Authors: Marijn Martens, Ralf De Wolf

Research Group: imec-MICT, Ghent University

Date: 29/05/2018

1 Preface

Edward Snowden's testimony about the PRISM program has clarified the intense and widespread practice of surveillance on the Internet and social media by governments. The leaked documents provided by Snowden indicated how the PRISM program had access to users' data from various ICT companies, such as Facebook, Google, Microsoft, and Apple. According to the whistleblower, the NSA further "impersonated Facebook in an attempt to trick users into downloading malicious code in its attempt to install malware on millions of computers which gives NSA control over users' computers" ("NSA posed as Facebook," 2014). The recent attack of the ransomware dubbed Wanna cry had victimisation rates of more than 200.000 computers in more than 150 computers and 10.000 organizations, it affected several hospitals, governmental agencies and private companies (Liptak, 2017). It took Equifax five months to report a hack into their servers that compromised 143.000.000 social security numbers that allowed hackers to pretend to be any of the victims in any given circumstance, such as the request of a new visa card (Lynley, 2017).

These are just some examples to show that citizens, businesses and governments are often targeted and impacted by what has been labelled as cybercrime. The booming of Internet technology (IT) creates many opportunities and permeates almost all aspects of our daily life (World Economic Forum, 2015). Today we live in a networked society with cloud computing, online transactions and other new interactions made possible by internet technology (Bendovschi, 2015). Unfortunately, IT also facilitates existing and new threats such as cybercrime (Tsakalidis & Vergidis, 2017). Cybercrime is an umbrella term for different online threats such as malware, scams, hacking and surveillance It can come as no surprise that cybercrime is growing globally (Interpol, 2017) given that estimated internet penetration of 2016 is up to more than 40% globally, for Belgium that is 88,5% (Internet live stats, 2017). This internet-penetration implies that more and more people are exposed to all the risks and threats that are inherent to the online world, cybercrime is one of them (Verdegem, Teerlinck & Vermote, 2015).

This study is part of a systematical investigation in Belgium about the costs and impact of cybercrime. The overall goal of this project is to assess the harms and costs of cybercrime on the government, industry and citizens. The latter insights substantiate and guarantee an evidence-based and effective cybersecurity policy, which, in turn, helps to defend all the involved parties.

Different research departments from the KU Leuven and the Ugent are involved in this project: the KU Leuven Centre for IT and IP Law (CiTiP) and the KU Leuven Institute of Criminology (LINC) as coordinator of the project, the KU Leuven imec-Distrinet Research Group, the KU Leuven imec-COSIC Research Group and the UGent imec-MICT.

The current study focusses on Belgian citizens and their online practices in order to describe the cost and impact of cybercrime. Specifically, we aim to demystify the process to protection and identify core target groups for risk communication by means of quantitative research. Our research consists of two separate but consecutive survey waves (as described in Work Package 3). The first wave of WP3 has been undertaken by imec-MICT as is the second and last wave. The first wave consisted of a large-scale quantitative survey (n=1033) which was conducted in the first quarter of 2015. The current wave consists of a follow-up survey in the last quarter of 2017 (n=1258). These two waves give us the possibility to compare results of the 2015 survey with the 2017 survey and thus compare the online practices of the average Belgian citizen over time.

The research leading to these results has received funding from the BRAIN-be research program of the Belgian Science Policy Office (BELSPO) under grant agreement number BR/132/A4/BCC. In addition, we would like to thank the different partners in the BCC-project for their input and support. Lastly, we want to thank the respondents who filled in our surveys.

Table of contents

List of Tables

Executive Summary

People who are **inexperienced in their internet** use are more susceptible to cybercrime and are typically unable to see if they have been victimized.

Pessimistic defensive internet users employ various security measures to protect themselves against cybercrime. They don't implement them effectively and still get victimized.

All but experienced internet users that are optimistic about the safety of the internet experience some kind of opportunity costs as a result of cybercrime.

More than 80% of the victimized people experienced **no direct costs** as a consequence of malware, hacking or monitoring. For scams, only 53.3% experienced no direct costs.

The implementation of **maladaptive security measures** (e.g., reduction or complete stopping of internet use or certain activities online) declined between 2015 and 2017.

The implementation of **adaptive security measures** (e.g. securing Wi-Fi networks, Checking the source and documents for anomalies) increased between 2015 and 2017.

The **perceived severity** of a cybercrime and the **perceived effectiveness** of the security measures are the strongest predictors for attitude towards taking security measures.

Subjective norm together with the attitude towards taking security measures especially explain the intention of taking this security measures.

2 Theoretical background

2.1 Cybercrime definition

2.1.1 Cybercrime in general

In academia and beyond there is no consensus about the concept of cybercrime and what it entails. Holt (2016) claims that the difficulty of defining cybercrime lies in the multidisciplinary context in which cybercrime resides. Some adopt the conceptualization in the justice system as a baseline to define cybercrime (Stratton, Powell, & Cameron, 2017). Others define cybercrime after the real-life counterpart (e.g. cyberstalking is defined as stalking in an online environment) (Henson, Reyns, & Fisher, 2016). Besides this, some researchers refer to the technical components of a specific threat when defining cybercrime (Van der Hulst & Neve, 2008).

In the BCC project we aim to include all the above-described components in an overall definition to be holistic and all-encompassing:

"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."

Computer-mediated activities are commonly divided into computer-*assisted* crimes and computer-*dependent* crimes, with the first being crimes that use the computer as a tool to do an already existing crime, and the second being a crime where the computer is the target (Europol, 2017). This division is widely accepted by policymakers and researchers (Li, 2016; Riek, Böhme, & Moore, 2016; Stabek, Watters, & Layton, 2010; Tsakalidis & Vergidis, 2017; Van der Hulst & Neve, 2008; European commision, 2007).

2.1.2 Typology

In the first wave, the typology of Anderson et al. (2013) and Holt & Bossler (2014) was used to further divide and categorize cyber threats. In the second wave, we fine-tuned the classification based on the results from the first and new insights of the Internet Organised Crime Threat Assessment and other recent research (Europol, 2017; Rens, 2015).

In our typology, we distinguish four types of cybercrimes; malware, scams, hacking and monitoring.

Malware is described as one of the key threats of cyber-dependent crimes, as are attacks on infrastructure and network attacks commonly known as hacking (Europol, 2017).

The two dominant **malware** threats are defined as ransomware and information stealers. We employ malware as the common nominator of viruses, ransomware and all software that alters the normal functioning of a device (Dang-Pham & Pittayachawan, 2015).

Scams are described as misleading actions to get information or money, in the context of cybercrime these scams use existing information technologies such as email and fake websites (Anderson et al., 2013).

Hacking is defined as unlawful or unauthorised access (Martellini, Abaimov, Gaycken, & Wilson, 2017; Verdegem, Teerlinck, & Vermote, 2015) and is linked to the key threat data breaches and network attacks by the Internet Organised Crime Threat Assessment (Europol, 2017).

In our typology of cybercrime, we also include activities that are considered illicit. Therefore **monitoring** was taken into account as a cybercrime even as this is not always the case from a legal point of view. In line with others we argue that the activity of monitoring in some occasions can be considered unethical and/or illicit (Dinev, Hart, & Mullen, 2008; Froomkin, 2015; Lyon, 2014; Verdegem et al., 2015).

This concludes in following definitions:

Malware is the malicious software that affects the normal functioning of your device.
E.g. virus, worms, Trojan horses, adware, botnets, ransomware…

A **scam** is an action whereby information or money is obtained by misleading a victim using information technologies.
E.g. via mail, false websites…

Hacking is obtaining unauthorized access to a computer or internet account.
E.g. Facebook, mail...

Monitoring is collecting data from a victim by the government or a private company.
E.g. checking internet usage, reading e-mails...

Our typology is neither exhaustive nor mutually exclusive. For example, scams and monitoring are often caused by malware and or hacking. Besides this it is also interesting to note that malware and hacking are both considered computer-dependent crimes, whereas monitoring and scams are considered computer-assisted crimes (Li, 2016, Riek, Böhme, & Moore, 2016; Stabek, Watters, & Layton, 2010; Tsakalidis & Vergidis, 2017; Van der Hulst & Neve, 2008).

2.2 Conceptualisation

2.2.1 Victimisation

Victimisation refers to the process and experience of being a victim of a crime (Paoli, Visschers, Verstraete, & van Hellemons, 2017). With some crimes, this is however not as straightforward as one might think. Much research solely takes into account the self-reporting of respondents to measure victimisation (Dodel & Mesch, 2017; Ngo & Paternoster, 2011; Rens, 2015), which, obviously does not include crimes that are unknown to the individual. On this topic Goucher (2010) argues that it is much more difficult for people to "defend themselves against an attack they may not recognise" (p.1). From a methodological point of view, self-reporting might lead to a bias and underestimation of victimisation.

For our conceptualisation, we follow the conceptualisation of victimisation of the veiligheidsmonitor (Centraal bureau voor statistiek, 2016). The veiligheidsmonitor is a monitoring tool used in the

Netherlands where they check -among other things- the victimisation of crime. They combine the victimisation of the individual with the victimisation of someone in your family.

2.2.2 Cost & Harm

Cost

It is important to have a general understanding of what one should understand as costs connected to cybercrime (Agrafiotis et al., 2016). In a systematic literature review of more than twenty studies that estimated the cost of cybercrime Wickramasekera, Wright, Elsay, Murray & Tubeuaf (2015) found no consensus about what should and should not be counted as a cost of cybercrime. Evidently, the measured costs were different in range across the studies. Anderson et al. (2012) differentiate between direct, indirect and defence costs.

Direct costs are the monetary equivalent of losses, damages, or other suffering felt by the victim as a consequence of a cybercrime.

Indirect costs are described as the monetary equivalent of the losses and opportunity costs imposed on society by the fact that a certain cybercrime is carried out, these include loss of trust and loss of opportunity.

Defence costs are the monetary equivalent of prevention efforts.

Anderson et al. (2012) division of the different costs was originally made to measure the total cost of cybercrime in response to the request of the UK Ministry of Defence to debunk overestimations of costs. After the study, they explicitly chose not to add up the different costs as this would show an opaque, context-free figure deemed meaningless (Anderson et al., 2013).

In contrast to the approach of Anderson et al. (2012), Paoli, Visschers, Verstraete and van Hellemons (2017)do not have the intention to quantify every cost of cybercrime. Harm is the direct non-quantifiable cost used in the framework of Greenfield and Paoli (2013) and is widely used as a concept by legislators of the EU.

The costs also differ depending on the perspective one adopts; the victim, government and society. (Wickramasekera, Wright, Elsey, Murray, & Tubeuf, 2015). Greenfield and Paoli (2013) distinguish four perspectives or potential “bearers of harm”, namely; individuals, private-sector entities, the government and the social an physical environment (Greenfield & Paoli, 2013). Every bearer has its own relevant “interest dimensions” where harm could be experienced. In this study, we measure the costs through the viewpoint of the victims. For individuals, this is functional integrity, material support, reputation and privacy and autonomy. We combined the categorisation of Anderson et al. (2012) and Greenfield and Paoli (2013) of these direct costs.

Lagazio, Sherif and Cushman (2014) proposed indirect costs as opportunity costs in their research. Additionally, a recent news release operationalized indirect costs as the opportunities someone lost because of security concerns (Eurostat, 2016).

We combine the classifications of Anderson et al. (2013), Paoli et al. (2017) and Lagazio et al. (2014) and differentiate between direct costs, opportunity costs and defence costs. Direct costs, however, are split into the direct monetary and direct non-monetary costs. Direct non-monetary costs are described using the harm assessment framework with the absence of material support as interest dimension (as this is seen as a direct monetary cost in this research). Under opportunity costs, we see the indirect costs as proposed by Lagazio, Sherif and Cushman (2014) and Eurostat (2016). Defence costs are the last category and defined as Anderson et al. (2013). Contrary to the research on the impact of cybercrime on Belgian businesses, we believe that citizens are able to estimate their spending on defence against cybercrime as their expenses are not bundled as in businesses (paoli et al., 2017). Indirect costs and defence costs are reported to be surprisingly high for cybercrime, which makes them of special interest (Anderson et al., 2013). We do believe however it is important to make a clear separation between the direct, indirect and defence cost to retain a transparent view of the costs.

Direct costs are the losses, damages, or other suffering felt by the victim as a consequence of a cybercrime.

> **Direct monetary costs** are the financial direct costs
>
> **Direct non-monetary costs** are the non-financial direct costs, considered as harm by Greenfield and Paoli (2013)

Indirect / Opportunity costs are described as the losses imposed by the fact that a certain cybercrime is carried out, these include loss of trust and loss of opportunity.

Defence costs are the financial costs of the prevention efforts.

2.2.3 Security measures

Adaptive vs maladaptive security measures

Academics have distinguished between adaptive and maladaptive security measures for different threats (Chou & Sun, 2017; Crossler & Bélanger, 2014; Jansen & Van Schaik, 2017; Verdegem et al., 2015). Adaptive security measures concern adequately protecting you against threats (Chou & Sun, 2017). In previous research, in the cybercrime context, this was described as protective measures like installing anti-virus software or changing security measures (Crossler & Bélanger, 2014; Verdegem et al., 2015). Maladaptive security measures, on the other hand, are about not protecting yourself adequately against threats (Chou & Sun, 2017). In previous research, this was described as the reduction or complete stopping of internet use or certain activities online (Verdegem et al., 2015). This can also be considered opportunity costs as individuals lose the opportunity to use certain internet tools because of fear of cybercrime (Eurostat, 2016).

Under adaptive security measures, we differentiate between social and technical adaptive security measures, respectively with a focus on social skills and technical skills needed to implement these security measures.

The **technical adaptive security measures** we take into account are:

- Installing free software
- Installing paying software
- Setting up software provided by operating system
- Updating software and operating system
- Securing Wi-Fi networks
- Using hard to guess passwords

The **social adaptive security measures** we take into account are:

- Checking the source and documents for anomalies
- Being critical when giving personal information to third parties

The **maladaptive security measures** we take into account are:

- Reducing/stopping internet usage
- Reducing/stopping certain activities online

2.2.4 Internet usage

Internet usage is most commonly conceptualised as the frequency of internet in academic research (Henson et al., 2016; Marcum, Higgins, & Ricketts, 2010; Ngo & Paternoster, 2011). Often, however, this frequency is combined with different kinds of activities online and devices used to do so. This approach allows researchers to have a more holistic view of the internet usages of individuals (Dodel & Mesch, 2017; Henson et al., 2016; Holt & Bossler, 2014; Leukfeldt & Yar, 2016; Reyns, Henson, & Fisher, 2011).

Our conceptualisation of internet usage has three sub-categories; frequency of internet use, number of devices used to do online activities and which activities are done online.

2.2.5 Perceived internet safety

Perceived risk is seen as the counterpart of perceived safety and can, therefore, be used as a way to conceptualise perceived safety (Riek et al., 2016). Perceived risk is already commonly used in other research about cybercrime (Hanus & Wu, 2016; Jansen, Veenstra, Zuurveen, & Stol, 2016; Riek et al., 2016). Some research assessed the confidence in security on the basis of two dimensions: optimism and pessimism (De Jonge, Van Trijp, Renes, & Frewer, 2007). We used this conceptualisation to measure the perceived safety of the internet in general. For the conceptualisation of the perceived safety of the different activities we followed other research that focused on comparing the perceived safety, they didn't divide between optimism and pessimism to keep everything comparable (Brownson et al., 2004; De Jonge et al., 2007; Verdegem et al., 2015).

2.3 Theoretical model: Protection Motivation Theory (PMT)

There has been a growing body of research trying to explain the overall risk of becoming victimized by cybercrime (Vakhitova, Reynald, & Townsley, 2016). Much of this work uses situational opportunity theories such as the lifestyle exposure theory, the routine activity theory or the lifestyle routine activity theory (Reyns, Randa, & Henson, 2016; Vakhitova et al., 2016). These studies are trying to expose the predictors to the chance of being victimized. Reyns et al. (2016) and Verdegem et al. (2015) argue that there is, however, little known about why people would have a higher or lower intention to perform security-related behaviour to counter these risks of being victimized.

In this study, we use the protection motivation theory (PMT) as our theoretical framework to understand people's intention to perform security-related behaviours (Rogers, 1975). PMT is a cognitive model that predicts behaviour, it is used in a wide range of research domains but was originally developed to explain how to influence risky behaviour in health research (Milne, Sheeran, & Orbell, 2000).

More recently, however, the PMT has been used in the context of cybercrime, where it is used to predict the motivation for protection or protective behaviour and to explain how to influence risky behaviour (Dang-Pham & Pittayachawan, 2015; Hanus & Wu, 2016; Herath & Rao, 2009; Jansen, Veenstra, Zuurveen, & Stol, 2016; Meso, Ding, & Xu, 2013; Safa et al., 2015; Shillair et al., 2015; Sommestad, Karlzén & Hallberg, 2015; Vance, Siponen, & Pahnila, 2012). PMT has even been used in the context of information security policy as well (Sommestad, Karlzén, & Hallberg, 2015). This model is thus ideal for the scope of this research as we try to demystify the process of the intention to take security measures and identify core target groups for risk communication.

According to the PMT, the cognitive mediating process to the attitude towards behaviour consists of two sub-processes, threat appraisal and coping appraisal (Jansen et al., 2016).

Threat appraisal is the cognitive process by which an individual evaluates the severity of the threat (=perceived severity) and the likelihood of being victimized by a certain threat (=perceived vulnerability) (Jansen et al., 2016). **Coping appraisal** is the cognitive process that answers the question if an individual feels him-/herself able to perform a certain security behaviour (= Self-efficacy) and the question if this security behaviour is effectivity to protect the individual against harm (=Response efficacy) (Jansen et al., 2016).

Awareness was introduced in the PMT model by Hanus and Wu (2016), they conceptualised awareness in two distinctly different groups namely threat awareness and coping awareness. They found a positive relation between threat awareness and perceived severity and between coping awareness and self-efficacy and response efficacy. There was no relation found between threat awareness and perceived vulnerability (Hanus & Wu, 2016).

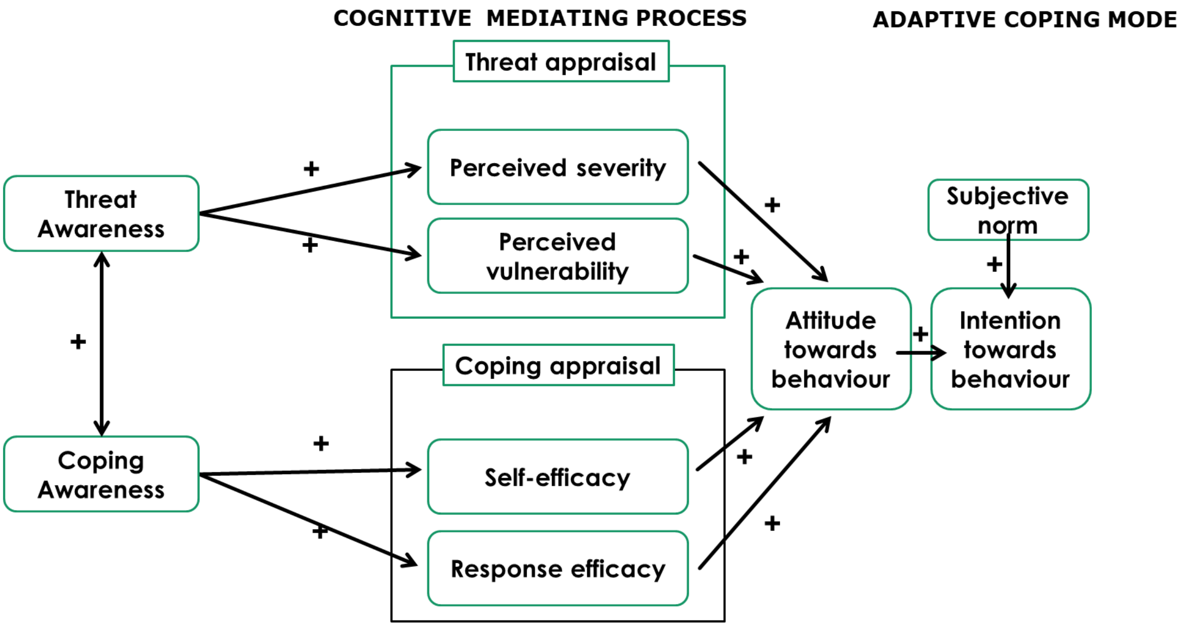


Figure 1 PMT-model

We expect all these variables to have a positive relationship with the attitude towards behaviour (Sommestad et al., 2015). Moreover, we assume that threat awareness and coping awareness in their turn have a positive correlation with one another and with perceived severity, perceived vulnerability, self-efficacy and response efficacy as modelled and tested by Hanus and Wu (2016). Furthermore, we expect that attitude towards behaviour and subjective norm have a positive correlation with the intention towards behaviour itself as modelled and tested by Tsai et al. (2016) and Verdegem et al. (2015). Subjective norm is seen as the perceived social pressure to engage or not in a certain behaviour and is expected to have a positive influence on intention towards behaviour (Verdegem et al., 2015).

2.4 Research questions

The overall goals of the first and second wave are as follows:

- 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
- To deepen the understanding of the different sorts of cybercrimes, their occurrence and how they are handled with
- To develop a risk perception monitoring tool to identify and describe factors associated with the public's intention to adopt protective measures
- To formulate recommendations considering risk communication efforts related to cybercrime

To achieve the above-defined goals the following research questions are central to this study:

RQ1: What is the state of the general Belgian population in terms of victimisation, security measures and costs of cybercrime?

> RQ1.1: How have victimisation rates, security measures and the costs of cybercrime evolved between 2015 and 2017?

RQ2: What are the different types of groups of Internet users and their security-related behaviour?

> RQ2.1: Which type of users are the most vulnerable?
>
> RQ2.2: How has the typology evolved between 2015 and 2017?

RQ3: What are the costs connected to cybercrime as experienced by the average Belgian citizen?

> RQ3.1: How have the perceived costs evolved between 2015 and 2017?

RQ4: What are the predictors of the public's intention to adopt protective measures?

3 Method

In what follows we will give you more information about the sample used in this research, furthermore, we will explain how we operationalized the different measures and describe the procedure of this research.

3.1 Sample

Our sample consists of 1258 valid responses and was recruited with representativeness for age, gender and residence in mind. In our analysis, we weighed our sample with a maximum of 1.37.

3.1.1 Distribution by gender

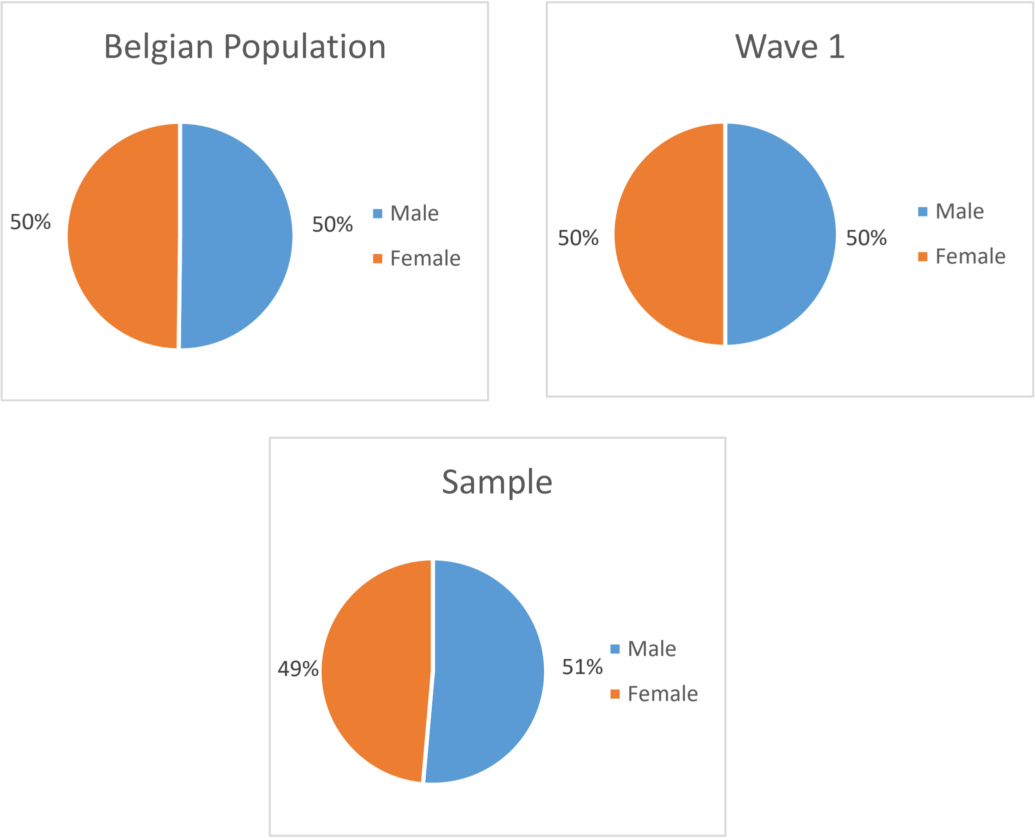


Table 1 Distribution by gender

Our sample almost consists of an equal amount of woman and men (see table 1).

3.1.2 Distribution by age

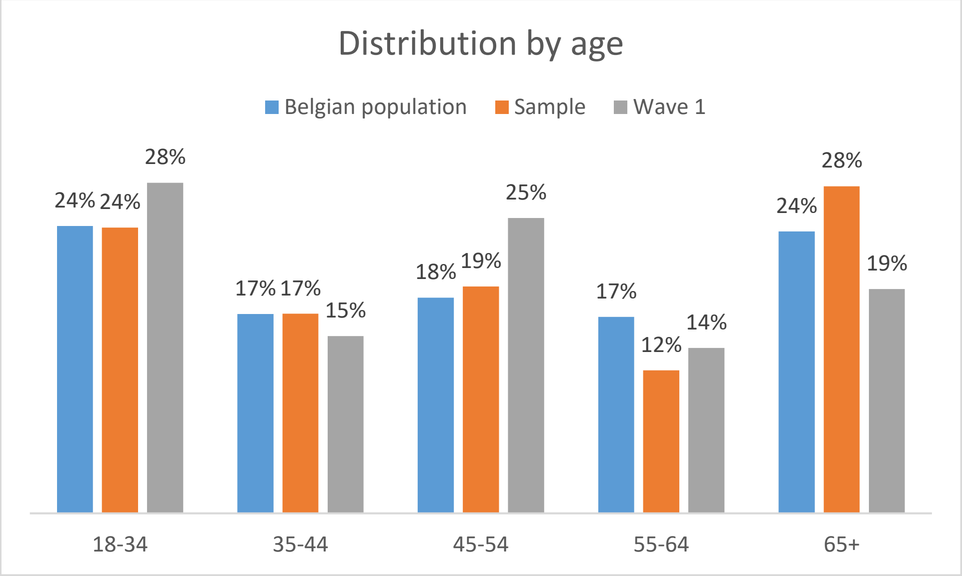


Table 2 Distribution by age

The ages of the respondents of our sample range from 18 to 89. The average respondent is 50 years old (M=49.97, SD= 16.24). If we compare our distribution by age with the one from the first wave we can see that we have significantly more 65+ people (p<.001), however the percentage of people in Belgium who are 65+ lies in between (see table 2). For further analysis, we weighed on the age groups to counter for the small inconsistencies between our sample and the general Belgian population.

3.1.3 Distribution by residence

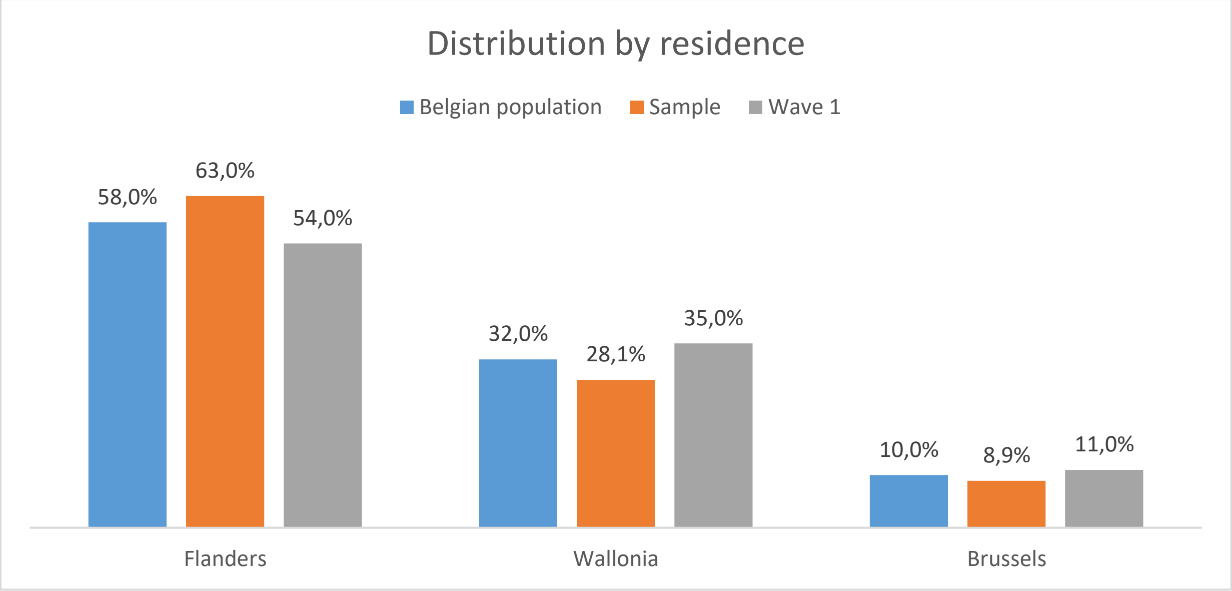


Table 3 Distribution by residence

In our sample, there is a small overrepresentation of people living in Flanders and a small underrepresentation of people living Wallonia and Brussels (see table 3). In comparison with the previous wave, we have significantly more people from Flanders (p<.01) and less from Wallonia (p<.01), there is no significant difference for Brussels.

3.1.4 Distribution by education level

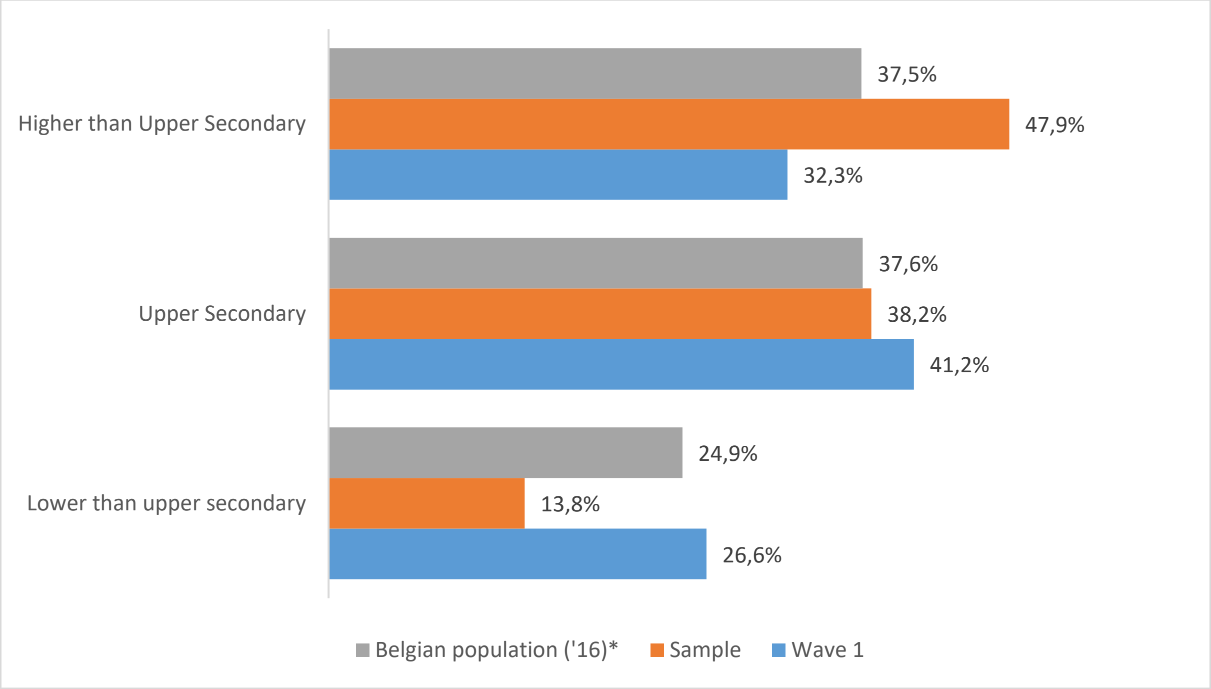


Table 4 Distribution by education level

*The data from the Belgian population is measured for 25 – 64-year-olds (OECD, 2017)

Table 4 shows us that our sample consists of mostly Bachelors or Masters (47.9%). The second largest lump are respondents who completed their higher secondary (38.2%). Almost 14% of our sample didn't complete their higher secondary education. We have more highly educated people in our sample than we had in the first wave or the Belgian population.

3.1.5 Distribution by employment situation

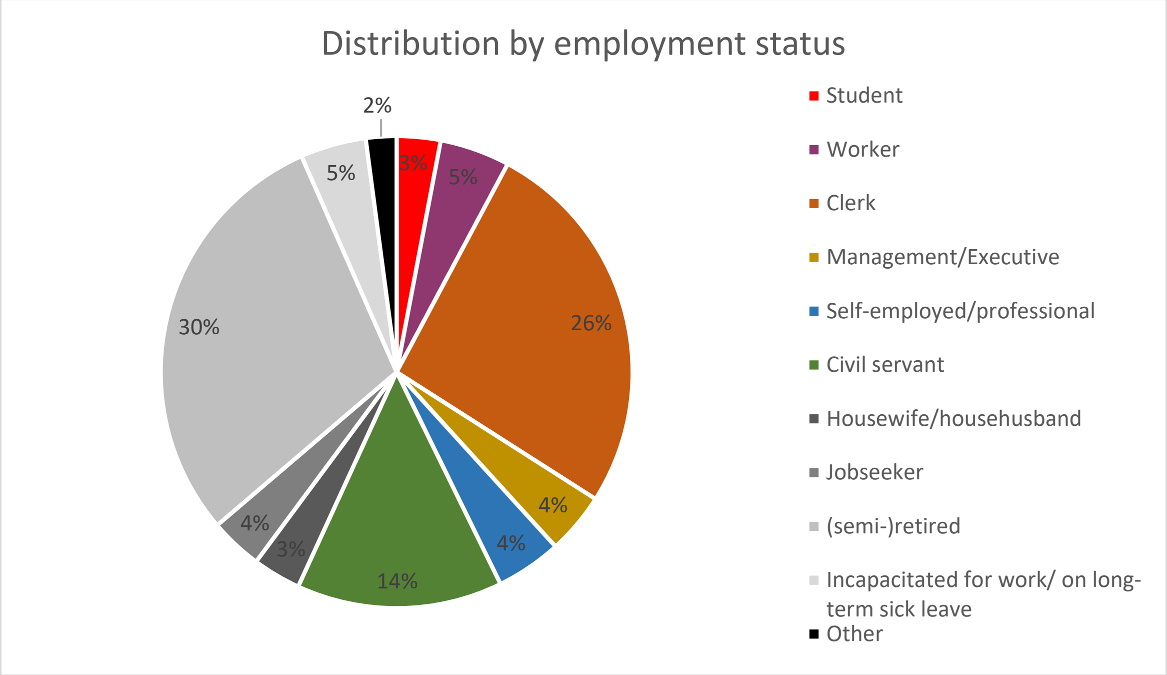


Table 5 Distribution by employment situation

In table 5 we can see that most of the people in our sample are professionally active (the coloured slices, 54%). This group consists of workers, clerks, management positions, professionals and civil servants. Almost one-third of the sample is (Semi-) retired (29.6%). This is in line with expectations as there is an overrepresentation of the age-group 65+ (see table 2). Most of the professionally active people in our sample are clerks (26%) or civil servants (14%).

3.1.6 Distribution by family situation

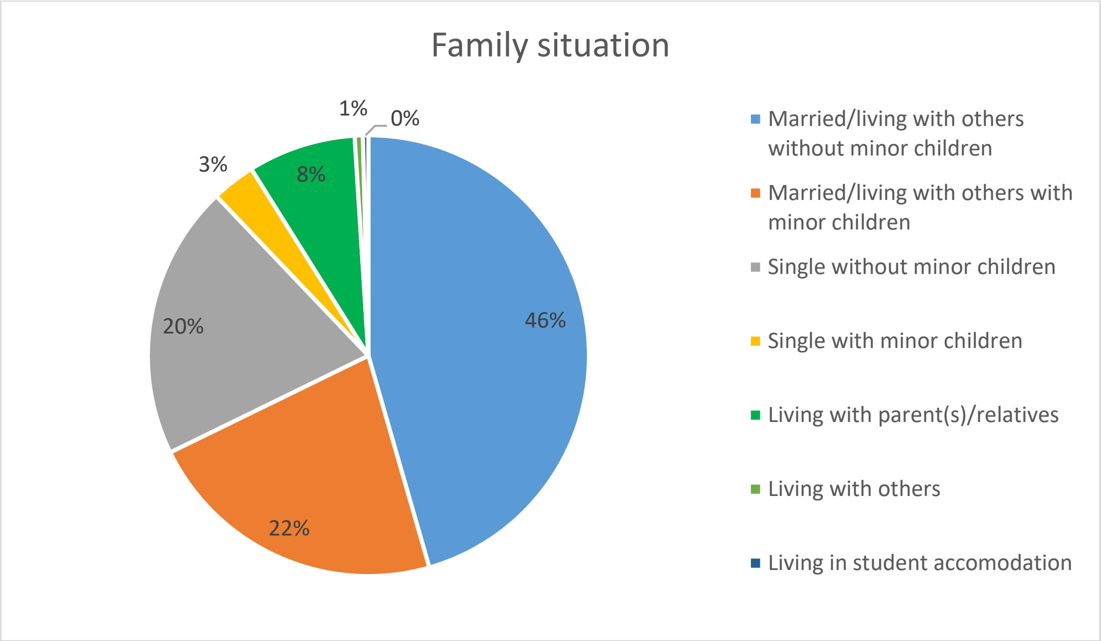


Table 6 Distribution by family situation

Table 6 shows the distribution of our sample by family situation, the biggest part of our sample is living with other people (80%). 46% is married or living with their partner without minor children, 22% lives with their partner and minors. 20% of the people in our sample lives alone.

3.2 Measures

In this section, we operationalize the concepts as described and delineated in section 2.2. All scales that are mentioned were rated on a 5-point Likert scale if not otherwise stated, ranging from "totally disagree" to "totally agree". In some occasions, the option "I don't know (it)" was added to prevent bias. Reliability of the scales was measured using Cronbach's alpha. If not stated otherwise we didn't change the operationalization of the first wave. For a full overview of all questions, we refer to appendix A.

3.2.1 Demographics

The first set of questions asked the respondents for their demographic information. We measured the respondents' gender, age, language, residence, profession, diploma and family situation. We preserved all of the questions from the first wave. Demographics were mainly used to check the representativeness of the sample and descriptive analyses.

3.2.2 Online activity

Different components of online activity were measured; access to certain devices, the uses of these devices, the location where respondents are online, and the frequency of internet use and the frequency of different online activities. The measures are based on the first wave (Verdegem et al., 2015). We did add some categories to get more fine-grained responses (for example, we added to category "between 5 to 8 hours" when measuring their internet frequency).

3.2.3 Awareness

To operationalize awareness, we differentiated between awareness of cybercrime and awareness of security mechanisms, as was recommended by Hanus & Wu (2016). Every concept was questioned on a five-point Likert scale ranging from "totally not aware" to "totally aware".

3.2.4 The perceived security of the internet and internet-related activities

The confidence and perceived security of the internet in general and specific internet-related activities were operationalized in line with previous work of Verdegem et al. (2015) and de Jonge et al. (2007). The former addresses the perceived optimism and pessimism about the security of the internet and combines these concepts into the perceived security of the internet. For the latter, we asked how safe they perceived various online activities ranging from "not safe at all" to "very safe".

3.2.5 Cybercrime victimisation

We based the operationalization of victimisation on the yearly in-depth monitoring tool of the Netherlands (Veiligheidsmonitor, 2017). In this monitoring tool, the victimisation of a respondent is the victimisation of themselves or someone in their household in the last 12 months.

Some questions were only asked at reported victims of cybercrime such as the direct costs monetary and non-monetary (cfr. supra) and reporting of the crime.

3.2.6 Cybercrime cost

Four different types of cost were operationalized; namely direct monetary cost, direct non-monetary cost (~harm), opportunity costs and defence costs.

In line with Verdegem et al. (2015) we operationalized direct monetary costs as an open question where we asked about the financial costs as a direct consequence of a certain.

To measure the direct non-monetary costs we used the operationalization of the harm assessment framework (Greenfield & Paoli, 2013; Paoli et al., 2017). The direct non-monetary costs included in our study are three-fold: daily activities, privacy and reputation. Harm was operationalized as a 6-point scale going from "harmless" to "catastrophic". We included the option "does not apply" to prevent bias. These questions were only visible to those who stated they were victimized in a previous answer.

Opportunity costs are measured using three techniques. Firstly, we have the direct questions that measure opportunity costs against online banking, online shopping and the use of social network sites (Eurostat, 2016). Secondly, we have the maladaptive security measures who implicate opportunity costs (Chou & Sun, 2017; Crossler & Bélanger, 2014; Jansen & van Schaik, 2017). Finally, we calculated the correlation between the frequency of use of a certain activity and its perceived security. These questions were asked to all respondents and not only those who stated to be a victim.

Defence costs consist of the monetary equivalent of prevention efforts (Anderson et al., 2012). We operationalized defence cost like direct costs with an open question (Verdegem et al., 2015). Sometimes these costs are considered irrelevant to take into account to measure the cost of cybercrime as these would inflate the total amount and would sketch an image not true to life, this consideration is certainly relevant when talking about businesses or governments (Paoli et al., 2017). For other internet-users, however, the defence costs are seen as relevant as these could have an impact on the adoption and use of certain internet activities or internet as a whole. Therefore we chose to include defence costs in this wave. With these concerns, however, it is important to divide the total cost into these transparent chunks, namely direct monetary costs, direct non-monetary costs, opportunity costs and defence costs. The questions concerning the former two were asked at victims, the latter two were asked independently of their victimisation.

3.2.7 PMT model

The PMT model was used in the first wave as well and we retained the operationalization of the different constructs in the PMT model (Verdegem et al., 2015). We did, however, change the scope of the questions. In the first wave, all the PMT-questions were about cybercrime in general. We chose to diversify and – next to cybercrime in general – also include the questions for the independent variables of malware and of scams. Doing this we follow the recommendation by Marakas et al. (2007) that stated that the measures should fit the context being studied as good as possible. It also makes it possible to zoom in on two specific cybercrimes. We chose for malware and scams as these were the two crimes where people were respectively the most and least victimized from in the first wave (Verdegem et al., 2015). These crimes were furthermore the two cybercrimes that people were most aware of (Verdegem et al., 2015).

All the independent variables are validated in other research and all but awareness is already used in the previous wave (Dang-Pham & Pittayachawan, 2015; Hanus & Wu, 2016; Herath & Rao, 2009; Meso et al., 2013; Verdegem et al., 2015). We asked all the questions about the perceived severity and the perceived vulnerability for all the crimes separately but not for cybercrime in general. The questions about self-efficacy, response efficacy, attitude towards security-related behaviour, intentions to perform security-related behaviour and subjective norm, we asked for malware, scams and cybercrime in general. This way we were able to get finer grained information about all variables and not exaggerate with the amount of questions.

The dependent variable of the PMT-model is “attitude towards security-related behaviour”, we however also measured how the intention is to perform this security-related behaviour and if the subjective norm has an influence on this intention together with the attitude.

Independent variables included in the original PMT-model:

- **Awareness of cyber-threat**
- **Awareness of security measure**
- **Perceived Severity**
- **Perceived Vulnerability**
- **Response Efficacy**
- **Self-efficacy**

Dependent variables included in the PMT-model:

- **Attitude towards security-related behaviour**

Dependent and independent variables outside of the original PMT-model

- **Intentions to perform security-related behaviour**
- **Subjective Norm**

3.3 Procedure

In order to answer the research questions, the research group imec-MICT launched an online survey in the beginning of October 2017. The participants were recruited by iVox - a professional market research agency. An URL to the questionnaire was available for 3 weeks and incentives in form of gift vouchers were handed out to a number of randomly picked participants. A total number of 2132 people started the survey. Of these 2132 people, 1258 were retained after validation. This validation was done using three measures.

- The respondents needed to answer a control variable (“tick the box totally disagree”) correctly.
- They needed fill in the survey in a credible time-frame (>10 minutes)
- They needed complete 90% of the survey.
  - For analysis concerning the remaining 10% of the survey, the missing values were disregarded.

On average it took a respondent 19 minutes (trimmed mean) to complete the survey. Our sample is representative for age, gender and residence with a maximum weighing of 1.37[1]. In the questionnaire, we included the definitions of the cybercrimes with a follow-up question and didn’t let the respondent continue if they answered wrong on this follow up question. In addition, we included an interactive way so respondents could look up the definitions of every cybercrime by hovering over the term any

[1] This weighing was conducted to counteract the under- and overrepresentation of the age groups 55-64 and 65+. We weigh our sample to get a perfect distribution on age. The other variable are not severely under or overrepresented. The quota for representativeness are based on the statistics of BE.stat and OECD (FOD Economie, 2017).

time the term was presented in a question. We argue that these implementations further validate our research and its results.

To answer RQ1, RQ1.1, RQ2.1, RQ2.2, RQ3 and RQ3.1 we used descriptive and comparative analysis (χ^2-test, Mann-Whitney, Kruskal-Walis, Wilcoxon, One-Way Anova, t-tests, spearman correlation) dependent on the levels of data to answer our research question. Some analysis are done only on the victims of cybercrime, these analysis are exclusively explorative of nature and do not possess the power to be extrapolated to the Belgian population.

The clusters used to answer RQ2, RQ2.1 and RQ2.2 are constructed using PCA & Cluster analysis (just as in the first wave)

At last, we created a SEM-model to answer RQ 4 where we analysed the PMT-model and compared this between malware, scams and cybercrime in general. Furthermore, we ran a SEM-model for the model for different relevant clusters to get a better insight. To use the perceived severity and perceived vulnerability in the SEM model for cybercrime in general we made a sumscale of those items per cybercrime, as they were not asked for cybercrime in general. For cybercrime in general only malware, scams and hacking were included as monitoring is strictly not seen as a cybercrime (Dinev et al., 2008; Froomkin, 2015; Lyon, 2014). For the specific SEM-models for malware and scams, no sumscales were used.

The analysis was done using SPSS 24 and Amos 22, every analysis is checked for his/her assumptions, there were no violations found except when explicitly stated in the analysis.

4 Results

4.1 Victimisation, security measures and costs of cybercrime of the general population (RQ1)

In a first section we aim to answer the first research question as formulated in section 2.4.: "What is the state of the general Belgian population in terms of victimisation, security measures and costs of cybercrime?"

4.1.1 Online activities: activities undertaken & activity security

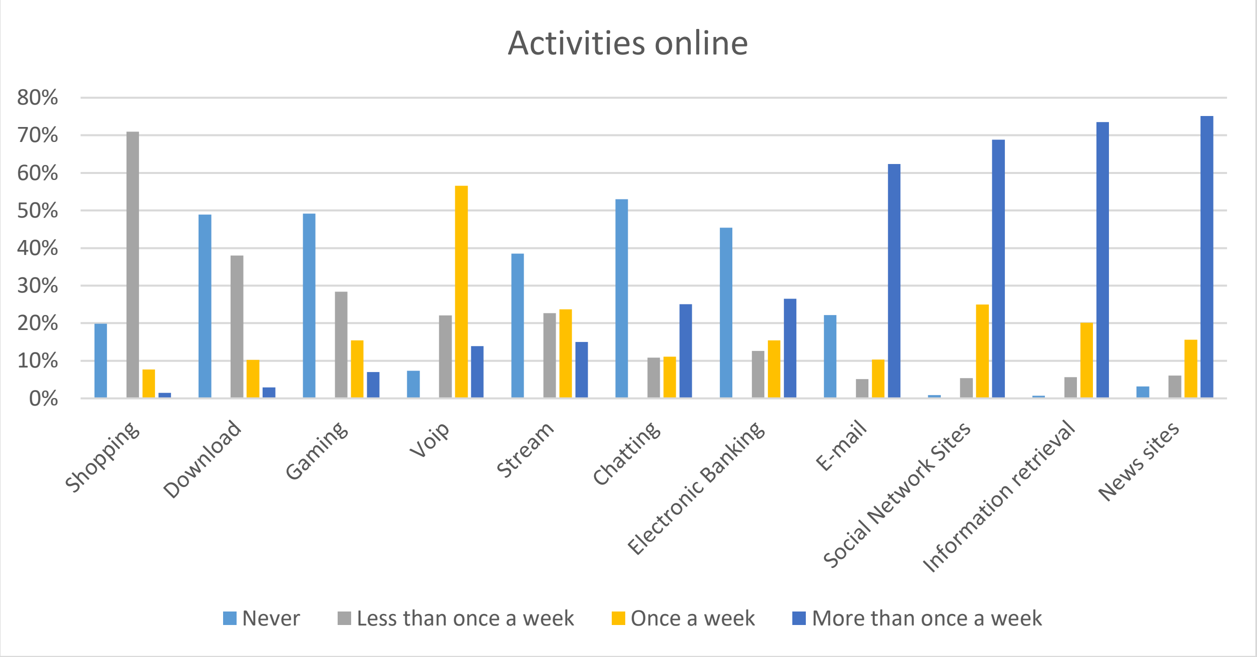


Table 7 Total sample: Online activities

Considering the activities one performs online we see a big difference between the frequencies of these activities (see Table 7). In our sample, the respondents score the lowest on online shopping. Moreover, many activities we included in this study are (almost) never performed. (e.g. Chatting, gaming, downloading, electronic banking). Checking E-mails, activity on Social Network Sites and retrieving information or consulting news sites are the most popular.

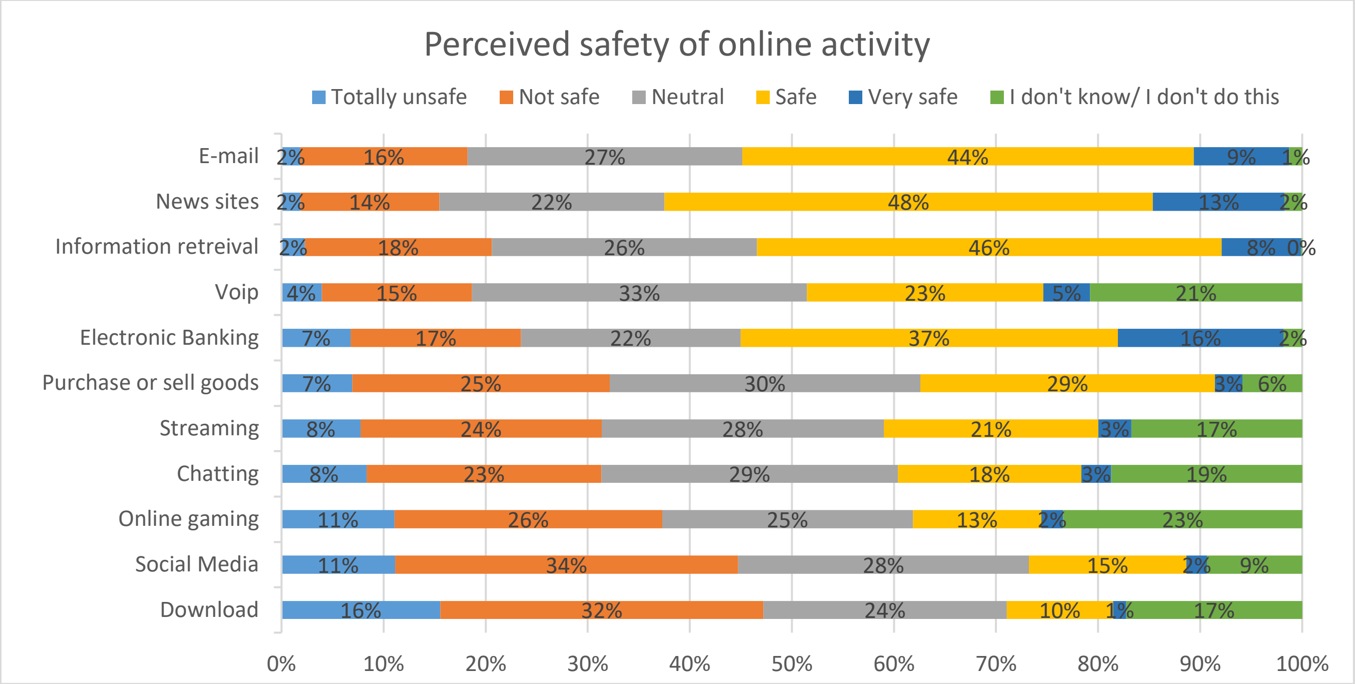


Table 8 Total sample: perceived security of online activities

If we take a look at the perceived security of a certain activity we can conclude that downloading is seen as the least safe activity (with most people stating it is totally unsafe) followed by social media, online gaming, chatting and streaming (see table 8). Interestingly is that for every activity at least 15% state that they find that activity "not safe" or less safe. In other words, every activity online is seen as somewhat unsafe by more than one in seven people. More than half (57.0%) of the people who do or at least know downloading, perceive it as "not safe" or less safe. Almost half of the people who use or at least know social network sites (49.3%) and online gaming (48.7%) also perceive it as "not safe" or less safe. Less than 20% of the population perceive Downloading, Social media or online gaming as "safe" or safer.

Less than 20% of the people perceive downloading, social media use or online games as at least safe

Furthermore, we can conclude that there is a big fraction of the population perceiving electronic banking (16.24%), visiting news sites (12.92%) and e-mail (9.35%) as very safe. It is also important to note that for some activities there is quite a big group of the respondents that didn't know or didn't perform the activity.

Correlations between online activity and perceived safety

After a two-tailed Spearman correlation between the perceived security of an activity and its frequency of use, we find that there are quite a few activities where this correlation is significant. Six of the activities have a significant correlation that is higher than .200 (see table 9). Hence, the higher their frequency of doing an online activity, the higher the perceived safety of that particular activity. Only for email and downloading this relation is not significant.

Activity	**Correlation coefficient**	**p**

Information retrieval	.077**	<.01
News sites	.125**	<.01
E-mail	.042	.054
Electronic Banking	.122**	<.01
Online gaming	**.356****	<.01
Social Media	**.266****	<.01
Chatting	**.308****	<.01
VoIP	**.274****	<.01
Purchase or sell goods	**.227****	<.01
Download	.052	.094
Streaming	**.287****	<.01

Table 9 Total sample: Correlations between online activity & perceived safety

This correlation could indicate opportunity costs as people who perceive a certain activity as less safe are performing this activity less often. Surprisingly this correlation is less strong for activities that are perceived safer like information retrieval, visiting news sites and electronic banking (cfr. Supra). Downloading and email, however, is not following this trend.

4.1.2 Security measures

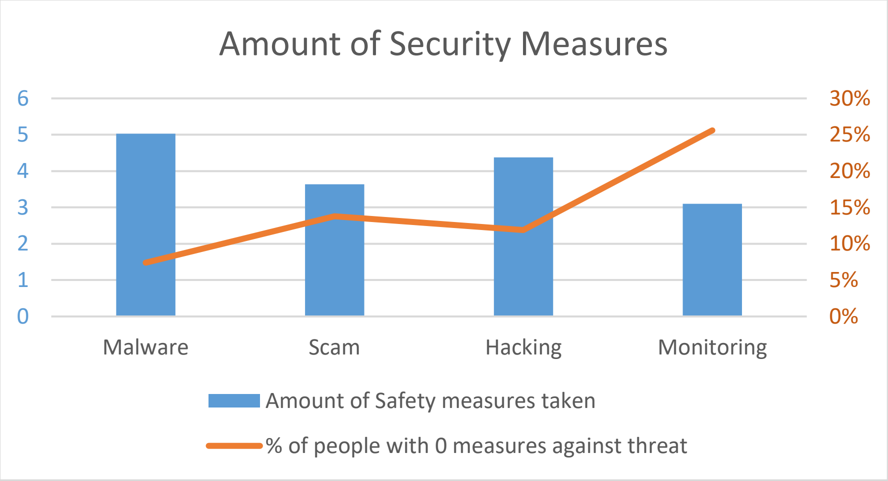


Table 10 Total sample: Amount of security measures taken

Analysing the number of security measures one takes we see that the most measures are taken against malware and hacking (see table 10). It is important to note that even with the lowest average amount of security measures being 3.09 security measures, there are for every crime between 7.4% and 25.6% that do not implement any of the proposed measures as a security measure. This makes them especially vulnerable to cybercrime. Interestingly more than one in four people do not take any security measure against monitoring, they do however averagely use more than three security measures to protect themselves against monitoring.

More than one in four people does not take any security measures against monitoring

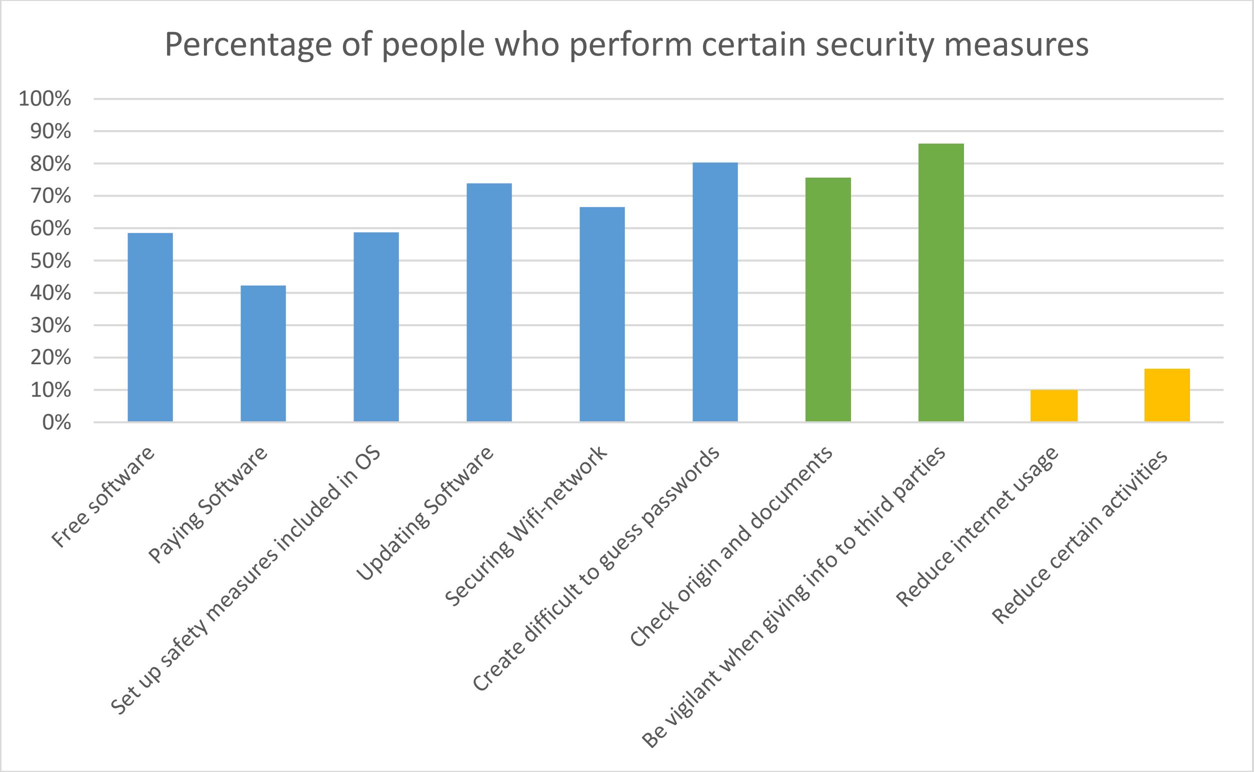


Table 11 Total sample: percentage of people who perform certain security measures

Almost 10% (9.7%) is reducing their internet usage and 16.5% is reducing or stopping certain activities online, these security measures are described as maladaptive and incorporate opportunity costs (yellow bars). In comparison with the other security measures this is much lower, but still more than one in ten Belgians are implementing a maladaptive security measure of any kind (see table 11).

More than one in ten people implement maladaptive security measures

Most people protect themselves by using social adaptive security measures such as checking the origin and documents before opening and being vigilant when giving info to third parties. It is however impossible to know if these social security measured (green bars) are applied in an effective way. This is dependent on the knowledge and skills of the person implementing these social adaptive security measures. If this is not the case, these social adaptive security measures will, of course, have no impact on the defence people have against cybercrime.

For every adaptive technical security measure (blue bars) - besides paying for software (42,3%) - the majority of people is using them. This means that less than 50% is willing to pay for their security measures. The recent trend of including security measures in operating systems for free is thus a good evolution and should continue.

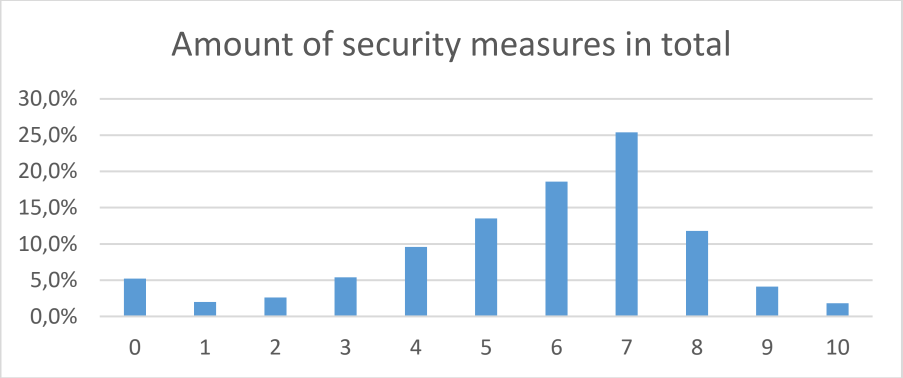


Table 12 Total sample: amount of security measures in total

With 84% of the people using four or more security measures and more than half using six or more security measures, most people are taking security serious (see table 12). There are however still 5.2% of the people who take no security measures whatsoever and more than 10% implementing two or fewer security measures.

More than 5% of the people implements no security measures at all

4.1.3 Victimisation

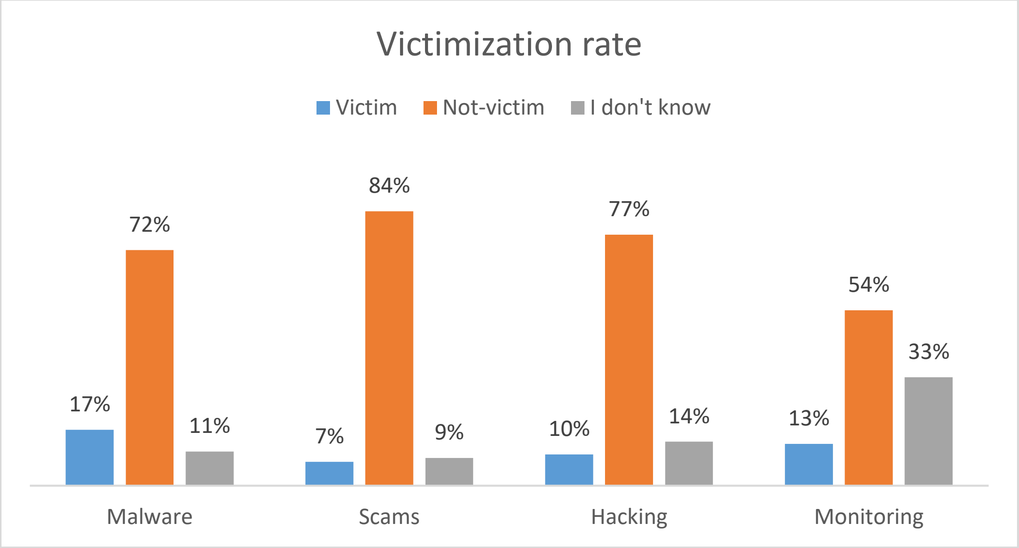


Table 13 Total sample: victimisation rate

With 17%, **malware** caused for the most victims the last 12 months (see table 13). People were least confronted with **scams**. The data also shows how most people are uncertain about **monitoring**. A total of 33% did not know if they were monitored or not by third parties.

Most victims were caused by malware in 2017

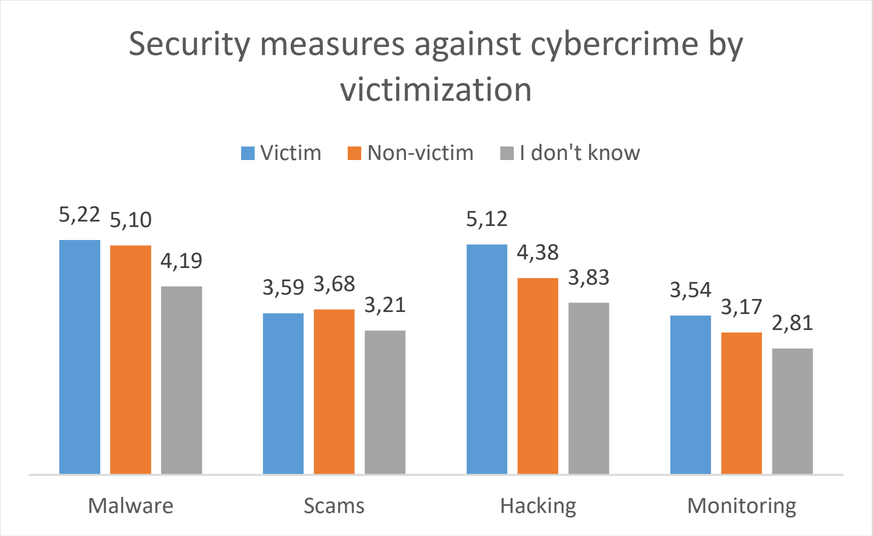


Table 14 Total sample: security measures taken against cybercrime by victimisation

A one-way Anova shows a difference between victims, non-victims and those who do not know if they are victimized by **Malware** considering their amount of security measures. (F(2)=9.068 p<.001) A post hoc analysis using Scheffe further indicates no significant difference between the victims and the non-victims. There is, however, a significant difference between the victims (M=5.2215 SD=2.28135) and the unknowing (M=4.1884 SD=2.92571) (p<.01) and the non-victims (M=5.1025 SD=2.36944) and the unknowing (p<.001) (see table 14).

Those who do not know if they were victimized implemented less security measures, this is true for three of four cybercrimes

There is no significant difference in security measures for **scams** between victims, non-victims and unknowing (F(2)=1.769, p=.171).

For **Hacking** there is a significant difference between all the groups (F(2)=8.895, p<.001) with the post hoc analysis using Scheffe showing that the victims are having significantly more security measures in place (M=5.1239 SD=2.52641) followed by the non-victims (M=4.3752 SD=2.54037) and then the unknowing (M=3.8253 SD=2.59582)[2].

For **monitoring** the one-way Anova with a post hoc using Scheffe also shows a significant difference between the victims (M=3.5407 SD=2.66390) and the unknowing (M=2.8110 SD=2.57896)(p<.05)(F(2)=4.876, p<.01), where the unknowing implement fewer security measures than the victims.

In three of the four cybercrimes the respondents who stated they didn't know if they were victimized implemented significantly fewer security measures than at least one other group. This makes this unaware group especially vulnerable.

[2] Victims vs non-victims (p<.05), Victims vs unknowing (p<.001), non-victims vs unknowing (p<.05)

4.1.4 Cybercrime Cost (RQ3)

Direct monetary cost[3]

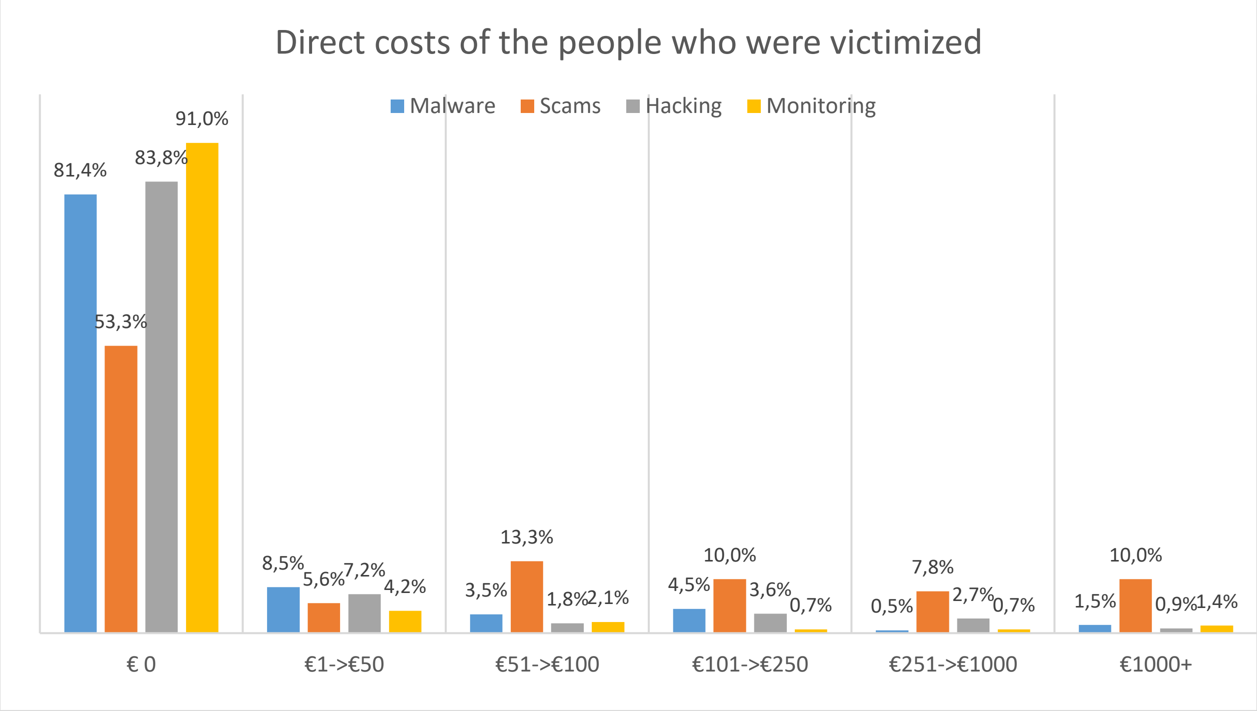


Table 15 Total sample: direct monetary costs by cybercrime

If we take a look at the monetary costs that are the direct consequence of a certain cybercrime, we can conclude that scams are the costliest of cybercrimes. More than 80% of the victims of malware, hacking or monitoring paid €0 as direct costs. 46.7% of the victims of scams, however, reported a direct cost of more than €0. 10% of the victims of scams even reported a loss of more than €1000. More than 25% of the victims of scams reported a loss of more than €100 (see table 15).

More than 80% of the victims of malware, hacking or monitoring paid €0 as a direct cost

In comparison, just 18.6% of the victims of malware, 16.2% of the victims of hacking and 9% of the victims of monitoring reported a direct loss of any amount.

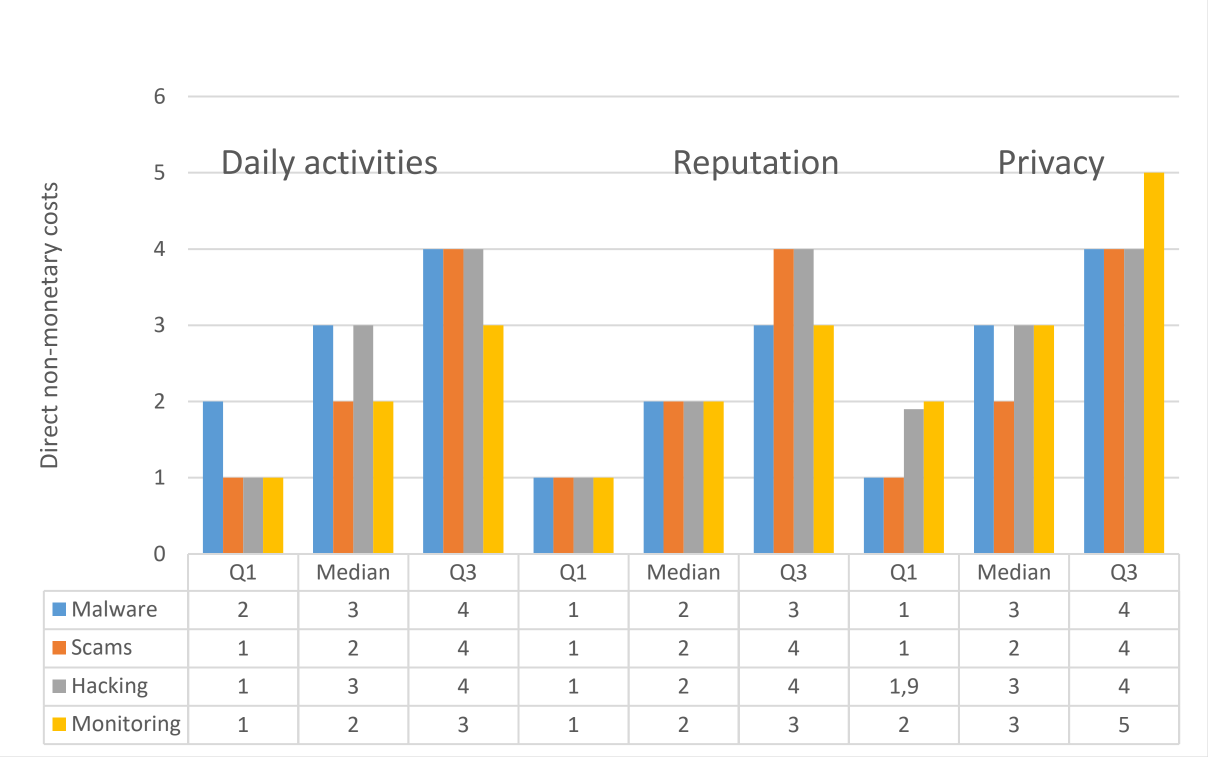
Of the victims of malware, only 6.5% stated a bigger loss than €100. Of the victims of hacking, this is 7.2%, of the victims of monitoring this is 2.8%.

Direct non-monetary cost

No significant differences were found when comparing the sumscale (malware: α=.886, scams: α=.915, hacking: α=.872, monitoring: α=.841) of the harm against daily activities, privacy and reputation for malware (M=2.6783 SD=1.32443), scams (M=2.5991 SD=1.42012), hacking (M=2.8775

[3] Averages are not being reported because the amount of respondents that paid direct costs is too low, with only 37 for malware, only 42 for scams, 18 for hacking and 13 for monitoring and because some outliers would influence the average too much.

SD=1.41128) or monitoring (M=2.5809 SD=1.30074). This means that the harm done by a cybercrime is perceived equally harmful for the different cybercrimes.



	Q1	Median	Q3	Q1	Median	Q3	Q1	Median	Q3
■ Malware	2	3	4	1	2	3	1	3	4
■ Scams	1	2	4	1	2	4	1	2	4
■ Hacking	1	3	4	1	2	4	1,9	3	4
■ Monitoring	1	2	3	1	2	3	2	3	5

Table 16 Total sample: direct non-monetary cost by cybercrime (1=harmless, 2=insignificant, 3=moderate, 4=serious, 5=grave, 6=catastrophic)

More than 50% of the victims of malware and more than half of the victims of hacking state that their **daily activities** were moderately or more harmed by the cybercrime (see table 16). On the other hand just more than 25% of the victims of monitoring state that monitoring has moderately harmed or worse their daily activities. If we look at **reputation** we see for more than 25% of the victims of scams or hacking this incident was perceived as a considerably harmful or worse for their reputation.

50% of all but the victims of scams state that they perceived the harm to their **privacy** as moderate or higher. For more than 25% of the victims of monitoring, this was even considered serious, for the other crimes more than 25% of the victims considered the incident as considerably harmful to their privacy.

Opportunity cost

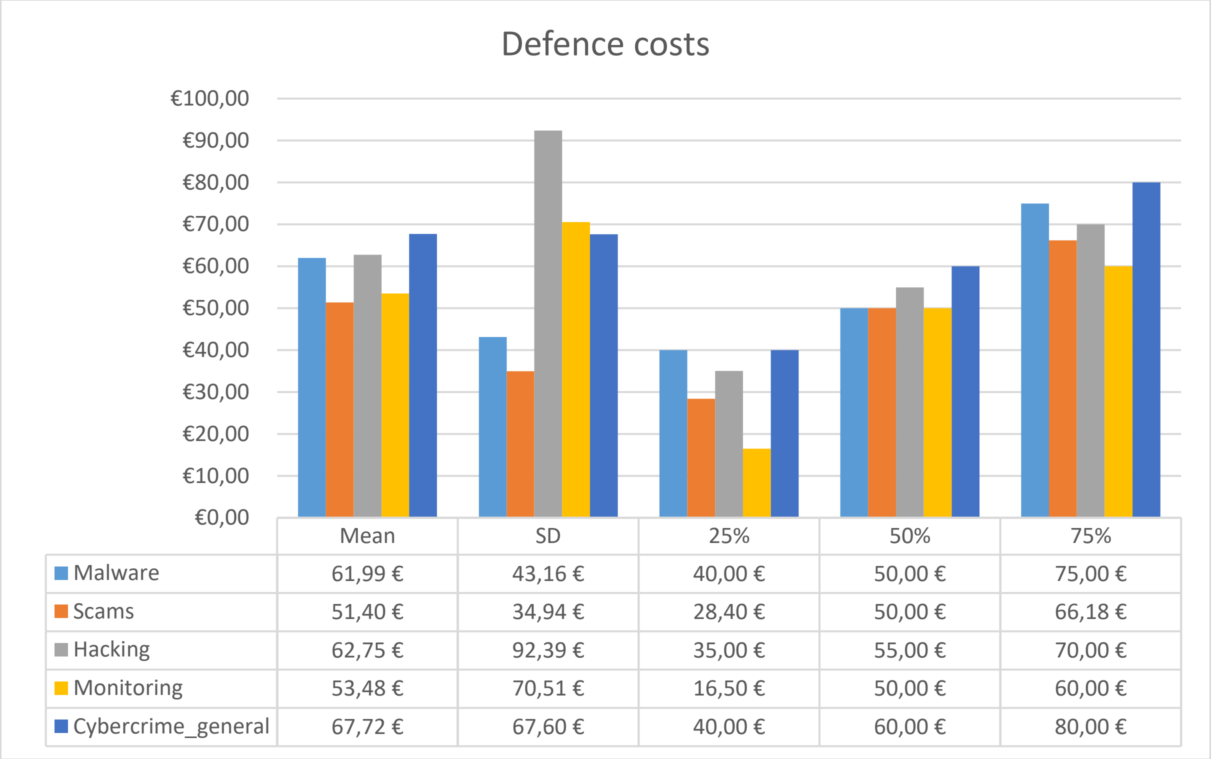
If we look at the direct questions about opportunity costs, 5.9% of the sample agrees that they reduced or stopped the use of electronic banking because of the threat of cybercrime. For online shopping, this is a higher 10.4% and for social network sites, this is 9%.

If we look at the maladaptive security measures we can see that 9.7% of the sample is reducing or stopping internet use as a security measure, even 16.5% of the population reduce or stop certain activities online as a security measure.

The correlations between the perceived security of a certain activity and its frequency of use shows us that there is quite a big opportunity cost as electronic banking (r=.122, p<.001), social network sites (r=.266, p<.001) and purchasing goods online (r=.227, p<.001) have a significant correlation, this combined with the direct questions about these activities makes us believe that people experience opportunity costs for these activities. Furthermore other activities such as online gaming (r=.356, p<.001), chatting(r=.308, p<.001), VoIP (.274, p<.001) or streaming (r=.287, p<.001) have an even stronger relationship between their frequency and perceived security.

The combination of these three methods gives us the insight that there is quite a big opportunity cost that people experience as a result of cybercrime.

Defence cost



	Mean	SD	25%	50%	75%
🟦 Malware	61,99 €	43,16 €	40,00 €	50,00 €	75,00 €
🟧 Scams	51,40 €	34,94 €	28,40 €	50,00 €	66,18 €
⬜ Hacking	62,75 €	92,39 €	35,00 €	55,00 €	70,00 €
🟨 Monitoring	53,48 €	70,51 €	16,50 €	50,00 €	60,00 €
🟦 Cybercrime_general	67,72 €	67,60 €	40,00 €	60,00 €	80,00 €

Table 17 Total sample: defence costs

If we compare the defence costs of the different cybercrimes we can see that malware (M=€61.99 SD=€43,16) and hacking (M=€62.75 SD=€92.39) are considered the most expensive (see table 17). Interestingly the median of all crimes is around €50. Which means that if someone pays for a defence against cybercrime, approximately half of them pay less than €50 and half of them pay more than €50, independent of the cybercrime. The costs of cybercrime in general are not much higher than the cost of the cybercrimes separately. It is likely that when people defend themselves against one crime, they also defend themselves against other crimes with this action.

4.1.5 Conclusion

In general, people are using the internet the most for information linked activities such as checking their emails, retrieving information, searching news websites and social networking. There is a clear positive relationship between the frequency of the different activities one performs online and the perceived security of those activities. Furthermore, we can conclude that people develop different

Scams made the least victims but cause the highest direct financial costs measures to protect themselves, not to say that these measures are adequate or effective. In general, most people were confronted with malware, followed by monitoring, hacking and then scams. Scams, however, caused for the highest direct financial cost linked to it.

Victims of hacking employ more security measures than non-victims. It is, however, difficult to know if they were victimized and as a result implemented more security measures or if they were victimized despite the security measures. Furthermore, it is important to conclude that in almost all cybercrimes the people who didn't know if they were victimized implemented fewer security measures compared to victims and non-victims.

Most victims do not experience direct costs as a consequence of an incident. Scams are the costliest of cybercrimes if it comes to direct costs. Almost half of the victims of scams state they've suffered direct monetary loss. Besides direct costs, there are many Belgian citizens who experience opportunity costs to some extent. These opportunity costs are felt in their online behaviour linked to the perceived safety of these activities but also in the maladaptive coping mechanisms implemented by more than one in ten people. Belgians spend most money defending themselves against malware and hacking. These are, however, not the cybercrimes with the highest direct costs. They are not stacking costs for different cybercrimes as most people pay money just once to defend themselves against all cybercrimes.

There are many Belgian citizens who experience opportunity costs

4.2 Typologies of internet users and their security-related behaviour (RQ2)

In a similar fashion to the first wave, we created clusters of people who share the same characteristics. This way we can have a better understanding of the practices of Internet users and their security-related behaviour. Following variables were used to differentiate in the typologies:

- Frequency of internet use
- Variety of internet use
- Variety of security measures
- Perceived security of the internet

Based on the analysis we differentiate between five groups:

- The optimistic defensive internet users (ODI)
- The pessimistic defensive internet users (PDI)
- The inexperienced unknowing internet users (IUI)
- The pessimistic experienced internet users (PEI)
- The optimistic experienced internet users (OEI)

In what follows we describe the different clusters in terms of general information which contains demographic information, their internet diet, their implemented security measures and their victimisation rate. Furthermore we compare this information and the costs and impact perceived by the different typologies. We can see that there are significant differences in age category (χ^2 (16) = 192.03, p<.001), residence (χ^2 (8) = 22.72, p<.01), gender (χ^2(4)=10.39, p<.05), education (χ^2(8)=32.40, p<.001) and profession (χ^2(40)=147.84, p<.001) for these different clusters. There is no significant difference found for the family situation (χ^2(12)=19.993, p=.067) between any of the clusters.

4.2.1 The Optimistic defensive internet user (ODI)

ODI - Passport

14.7%

Demographics

- Older (M=53 SD=14.8)
  - More 55-65 (p<.05)
  - Less 18-35 (p<.001)
- More from Wallonia (p<.05)
- More men/Less woman (p<.05)
- More (semi-)retired people (p<.05)

Internet diet

- Top tasks online
  - Visiting news sites
  - Searching information
  - Social network sites

Online perceived safety

- Internet as a safe place

Internet diet & perceived safety of online activities

If we take a look at the internet diet of an ODI, we can conclude that they mainly use the internet to visit news sites, as more than 75% of them does this at least once a day. Also searching the internet for information and email are done quite often – 75% of them does this at least once a week. They also use the internet for electronic banking and social network sites. Half of them use social network sites at least daily. Buying and selling goods online is rarely done, with half of them doing it at least monthly. The average ODI does not or to a lesser extend game, chat, use VoIP, download or stream.

The ODI's perceive the different activities online generally as neutral to safe, more than 75% perceive information retrieval, visiting news-sites, e-mail, electronic banking and Calling over the internet (=VoIP) as neutral or safer (see table 18). For the other activities there are still more than 50% that think those activities are "neutral" or safer. They are the only cluster where more than half of them perceive downloading as "neutral" or safer. Hence, this cluster is more optimistic about the Internet.

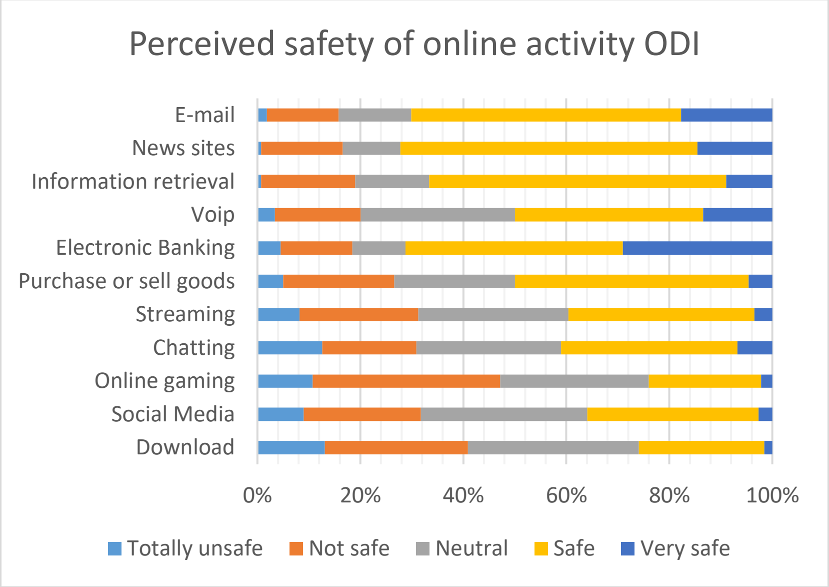


Table 18 ODI: Perceived safety of online activity

Security measures taken

If we look at the different kinds of security measures, we see that 10,2% of

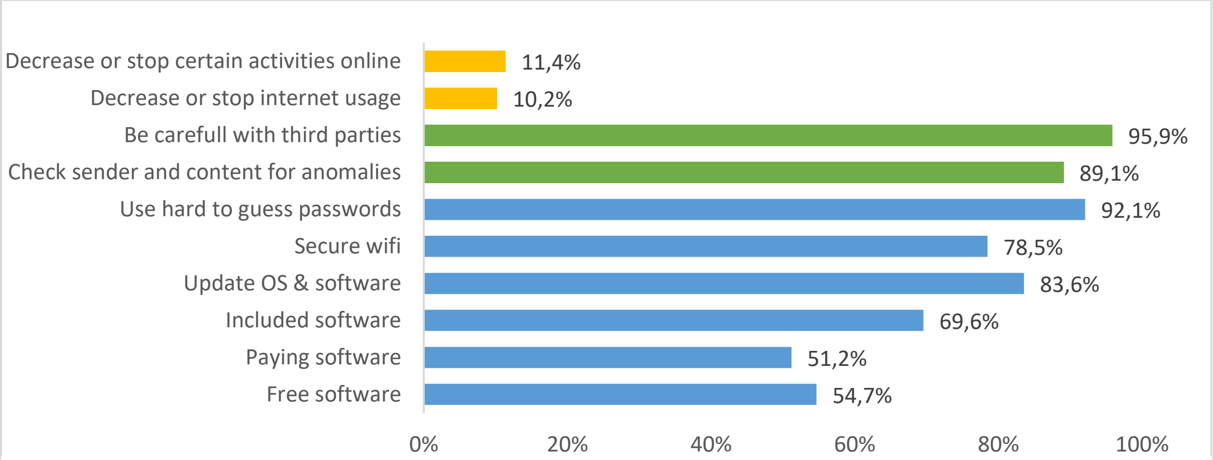


Table 19 ODI: Security measures taken

these users will reduce their internet usage in total and 11,4% will reduce certain activities online (see table 19). These maladaptive security measures are done least of the security measures but still more than one in ten ODI's misses opportunities in some way by implementing these maladaptive security measures.

There is a very high adoption of social adaptive security measures with 89,1% checking the origin and content for anomalies and 95,9% being careful when sharing content with third parties.

Also, adaptive technology security measures are adapted quite often by ODI's. With adoption rates ranging from at least more than half (51,3%) that pay for security software, to 92.1% who uses hard to guess passwords.

Victimisation rate ODI

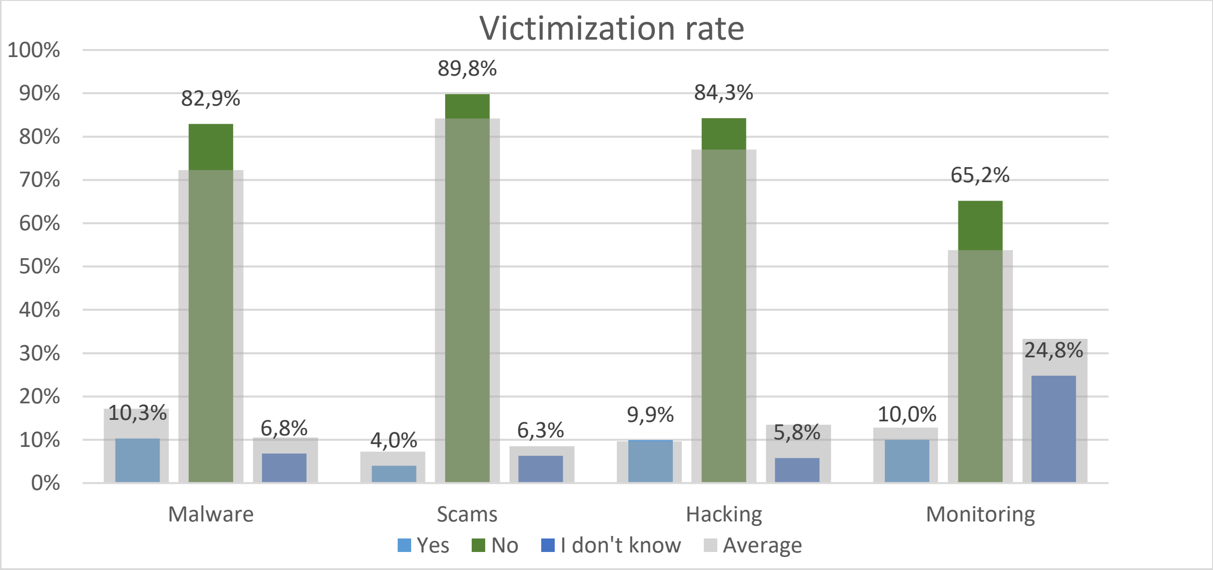


Table 20 ODI: Victimisation rate

Hacking (9,9%), malware (10,3%) and monitoring (10,0%) are the crimes from which most ODI's state that they (or someone in their family) were a victim of the last 12 months (see table 20). 24,2% of the ODI's state that they have been a victim of at least one of these cybercrimes. There are significantly less ODI's being victimized than expected by malware (p<.01) and significantly more not being victimized than expected by malware (p<.001) ($\chi^2(8)$=19.619, p<.05). There are also significantly more ODI's not being victimized by hacking than expected (p<.01) ($\chi^2(8)$=30.061, p<.001). The same is true for monitoring (p<.001) ($\chi^2(8)$=47.766, p<.001). We can thus conclude that ODI's are in general less victimized than one should expect.

The ODI's are in general less victimized than one should expect

4.2.2 The pessimistic defensive internet user (PDI)

PDI - Passport

23.4 %

Demographics

- Older (M=51 SD=14.2)
  - More 45-54 (p<.01)
  - Less 18-34 (p<.01)
- Lower education
  - More highest secondary degree (p<.05)

Internet diet

- Top tasks online
  - Sending & recieving email
  - Visiting news sites
  - Searching information
  - Social network sites

Online perceived safety

- Very low trust in the internet

Internet diet & perceived safety of online activities

The internet diet of the PDI's is very comparable to the one of the ODI's. With more than 75% of them sending & receiving emails and visiting news sites at least daily, at least 50% of them using social network sites at least daily, 75% of them retrieving information at least weekly, and 75% of them using electronic banking at least monthly, there is a big overlap in online behaviour. However in this cluster also more than half of them streams content at least monthly.

If we look at the perceived safety of the online activities we can clearly see that the PDI is perceiving the activities, in general, less safe than the ODI. More than 50% of the PDI's perceive online gaming, social media and downloading as "not safe" or less (see table 21). Only electronic banking, information retrieval, visiting news sites and e-mailing is perceived by more than 30% of the PDI's as "safe" or "very safe".

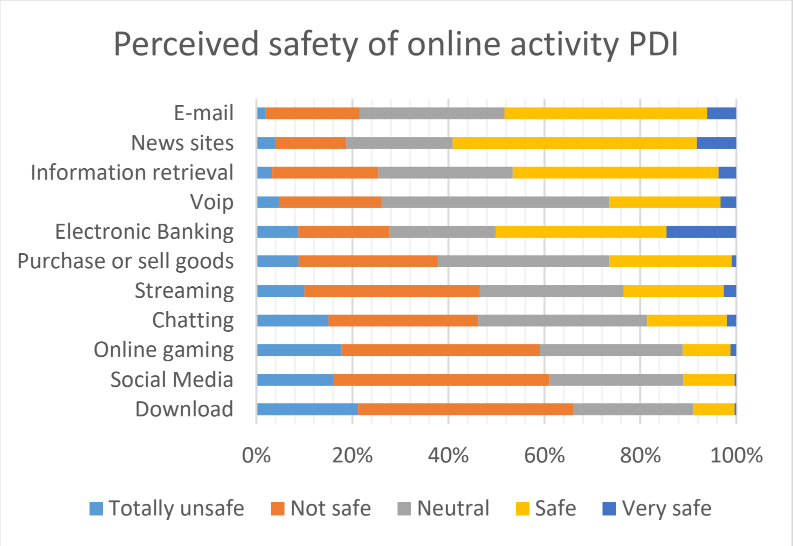


Table 21 PDI: Perceived safety of online activity

Security measures taken

There is not one respondent of the PDI's that has less than five security measures in place, this is to be expected as this is the group that is the most defensive of our sample. With an average of 7.10 security measures (SD= 1.27) they also have the highest average of security measures in place. They have most security measures in place to counter malware (Mean=7.05 SD=1.53) followed by hacking (Mean= 6.77 SD=1.54), scams (Mean=6.19 SD=1.76) and monitoring (Mean= 5.80 SD=2.15).

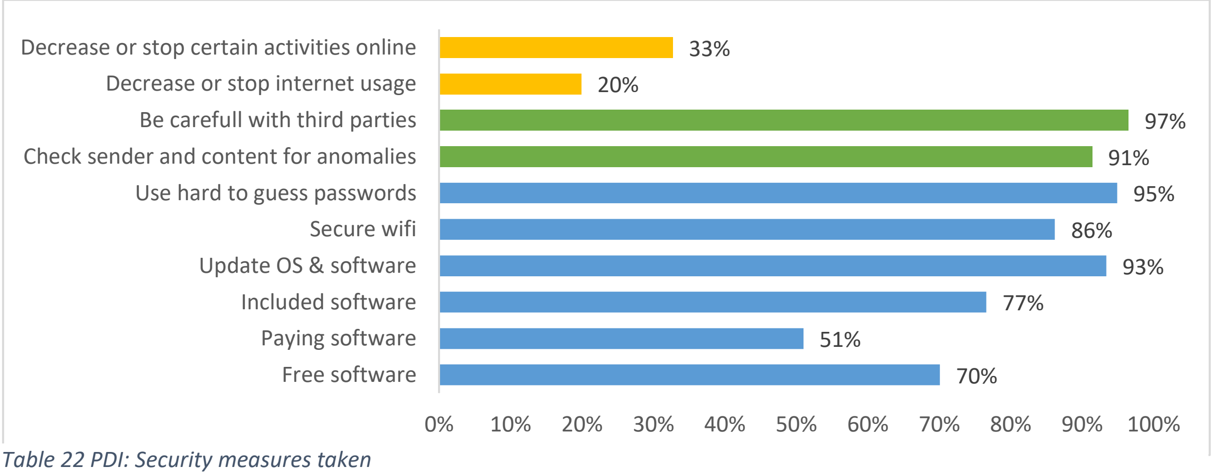


Table 22 PDI: Security measures taken

Striking is that there is also a big fraction of PDI's that apply maladaptive security measures such as decreasing or stopping internet usage (19.9%) and decreasing or stopping certain activities online (32.7%) (See table 22). This percentage is significantly higher than all the other clusters for reducing or stopping internet usage (p<.001)(χ^2(4)=50.752, p<.001) and reducing or stopping certain activities online (p<.001)(χ^2(4)=78.310, p<.001). These maladaptive security measures cause high opportunity costs for this profile.

Also, the adaptive security measures both social and technical are being heavily implemented by the PDI's. More than 70% is using free software to protect themselves and their families against cybercrime. An even higher 93.4% is trying to update frequently. One would expect that all these security measures would result in a lower victimisation rate.

Victimisation rate PDI

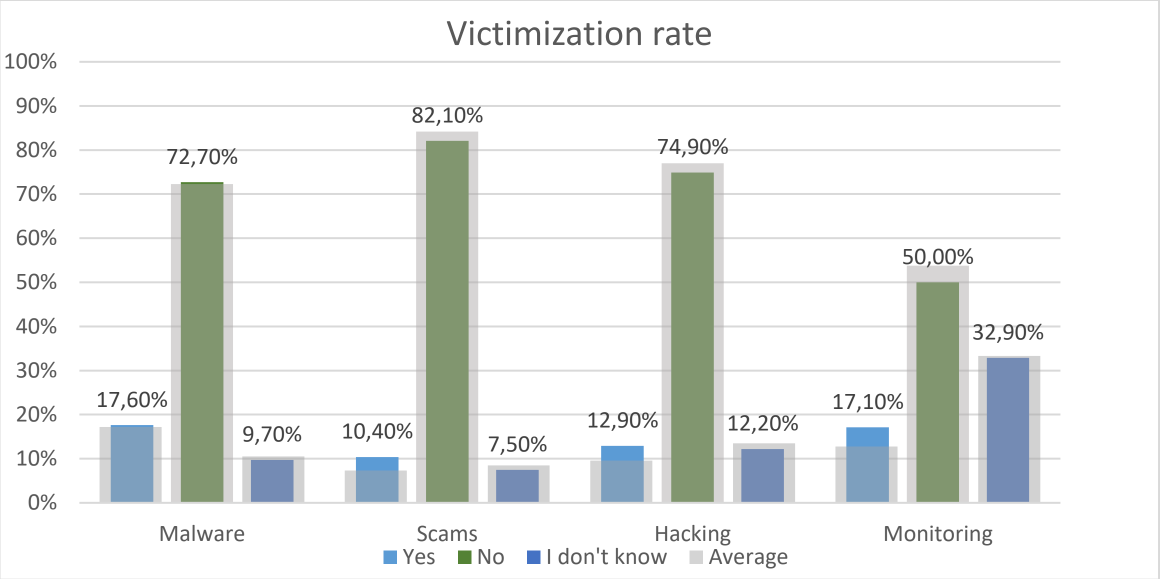


Table 23 PDI: Victimisation rate

This is however not the case, with malware (17.6%), monitoring (17.1%), hacking (12.9%) and scams (10.4%). There are overrepresentations of the PDI's that are victimized by hacking (p<.05)(χ^2(8)=30.061, p<.001) and monitoring (p<.05) (χ^2(8)=47.766, p<.001) (see table 23). 37.7% of the PDI's state that they or someone in their family have been the victim of at least one cybercrime last year.

37.7% of the PDI's state their family was victimized at least once last year

These findings could suggest that these PDI's are not implementing their security measures in a correct way, hence not in a way that is preventing them from being victimized.

4.2.3 Inexperienced unknowing internet user (IUI)

IUI - Passport

Demographics 24.9%

- Older (M=56 SD=15.00)
    - More 65+ (p<.001) & 55-65 (p<.05)
    - Less 18-34 (p<.001)
- Less white collar worker
    - Less clerks (p<.001) & management (p<.05)
    - More (semi-)retired (p<.001)
- Lower education
    - More highest secondary degree (p<.001)
    - Less at least a bachelor degree (p<.05)
- Less men/More woman (p<.05)

Internet diet

- Top tasks online
    - Visiting news sites
    - Searching information
    - Social network sites
- Less often than the rest (p<.001)

Online perceived safety

- Slightly less safe than average

Internet diet & perceived safety of online activities

The IUI's use the internet significantly less than all the other groups (p<.001). If they do use the internet, they use it mainly for information retrieval, visiting news sites and searching for information with 75% of them doing these activities at least once a week. Another part of their internet diet is electronic banking with 75% of them doing this at least monthly and social network sites with more than 50% of them doing this weekly. All the other activities are done yearly or never by 75% of the IUI's.

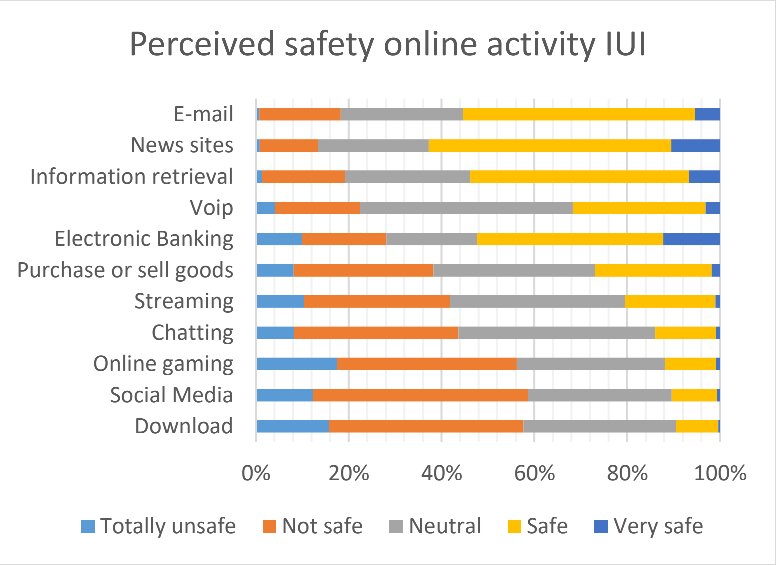


Table 24 IUI: Perceived safety of activity

They perceive the different internet activities mostly as "neutral" or "safe", especially the activities they perform online (see table 24). With more than half of them perceiving searching information, visiting news websites, emailing and electronic banking as at least "safe". Only online gaming, using social network sites and downloading are perceived as "not safe" or less by at least 50% of the cluster. The rest is perceived generally neutrally to safe. It is, however, important to know that the IUI have significantly more people not knowing what a certain online activity is or not doing a certain activity online (see table 33).

Security measures taken

The IUI's have by far the least security measures in place (Mean=4.28 SD=2.54). 13,7% of the cluster has no security measure in place whatsoever. With 19.8% of this cluster seeking no protection for malware, 33.1% seeking no protection against scams, 28.2% not protecting themselves against hacking and more than half (53.7%) not protecting themselves against monitoring, this cluster has a big group of vulnerable people. If they protect themselves it is more often than not with few security measures.

If we take a look at the different security measure, we can see that significantly fewer people from the IUI's are implementing free software (p<.01)(χ^2(4)= 36.823, p<.001), included software (p<.001) (χ^2(4)=96.639, p<.001), updating OS & Software (p<.001)(χ^2(4)=140.19, p<.001), securing Wi-Fi (p<.001)(χ^2(4)=136.807, p<.001), use hard to guess passwords (p< .001)(χ^2(4)=137.038, p<.001), check sender and content for anomalies (p<.001)(χ^2(4)= 125.470, p<.001) and are careful with third parties (p<.01) (χ^2(4)=101.898, p<.001) (see table 25). One should expect that with this security profile they would be victimized more often than the other clusters.

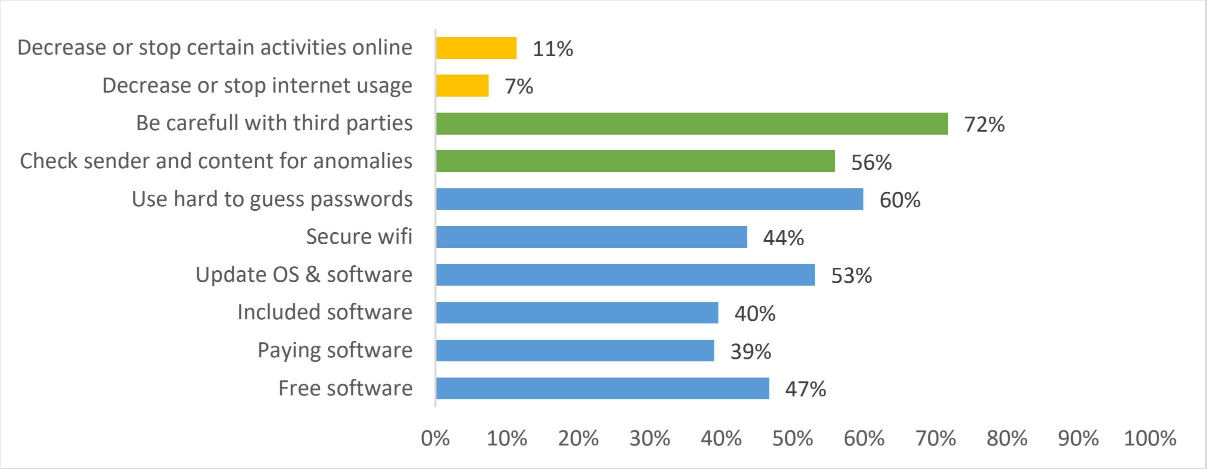


Table 25 IUI: Security measures taken

Victimisation rate IUI

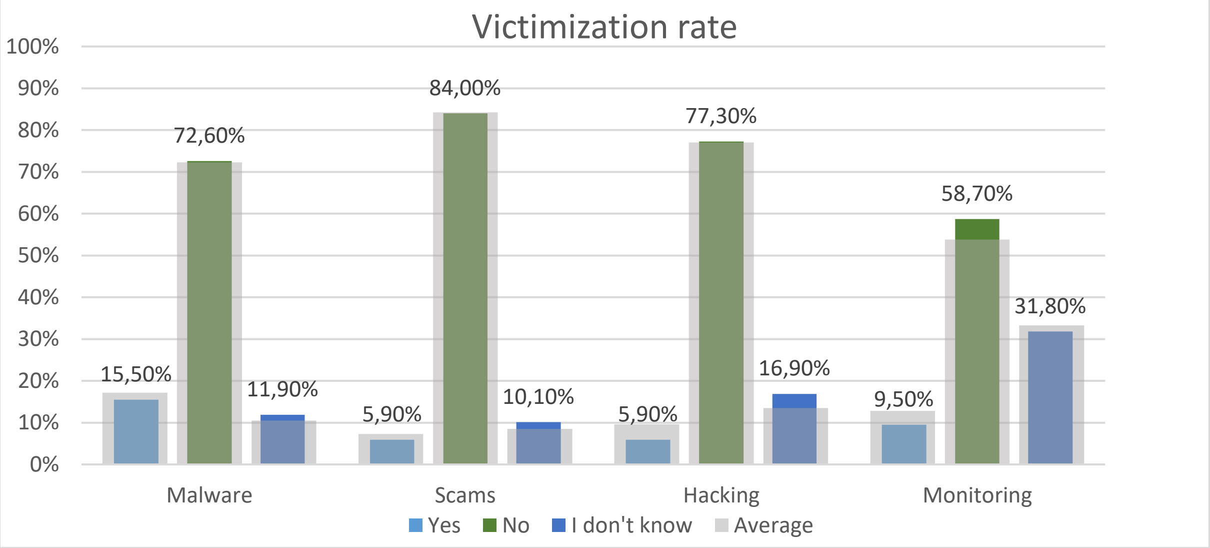


Table 26 IUI: Victimisation rate

Yet, if we look at the victimisation rate itself, there is no overrepresentation of the victimisation of any of the cybercrimes. There is even a slight significant underrepresentation of people victimized by hacking (p<.01)(χ^2(8)=30.061, p<.001) and monitoring (p<.05)(χ^2(8)=47.766, p<.001). Malware (15.50%), is just as in any other cluster the cybercrime where most IUI's were victimized followed by monitoring (9.50%), hacking (5.90%) and Scams (5.90%) (See table 26).

The low victimisation numbers of the IUI's could, however, be explained by the difference in internet diet and/or the possibility that they don't notice or are not able to notice if their computer is compromised (cfr. Infra).

4.2.4 Pessimistic experienced internet users (PEI)

PEI - Passport

20.0%

Demographics

- Younger (M=43 SD=14.85)
  - More 18-34 (p<.001)
  - Less 65+ (p<.001) & 55-64 (p<.05)
- More white collar worker
  - More clerks (p<.001) & civil servants (p<.05)
  - Less (semi-)retired (p<.01)
- Higher education
  - More lowest Bachelor degree (p<.001)
  - Less Highest secondary degree (p<.01)

Internet diet

- Top tasks online
  - Information tasks
  - Social tasks
  - Electronic banking
- more often than the rest (p<.001)

Online perceived safety

- Doesn't trust the internet

Internet diet & perceived safety of online activities

The PEI's use the internet on the one hand for traditional tasks such as email, searching information and visiting news sites. More than 75% of the PEI's do these activities at least once a day. On the other hand, they use the internet for social tasks such as social networks, with more than half doing this more times a day or chatting with more than half doing this at least once a week. Also, electronic banking is done often with more than 75% using it at least monthly as is streaming with half of them doing this at least weekly. Gaming, selling and buying goods, VoIP and downloading are still done at least once a year by more than 50% of the PEI's.

The internet diet of the PEI's resembles heavily the one of the OEI's.

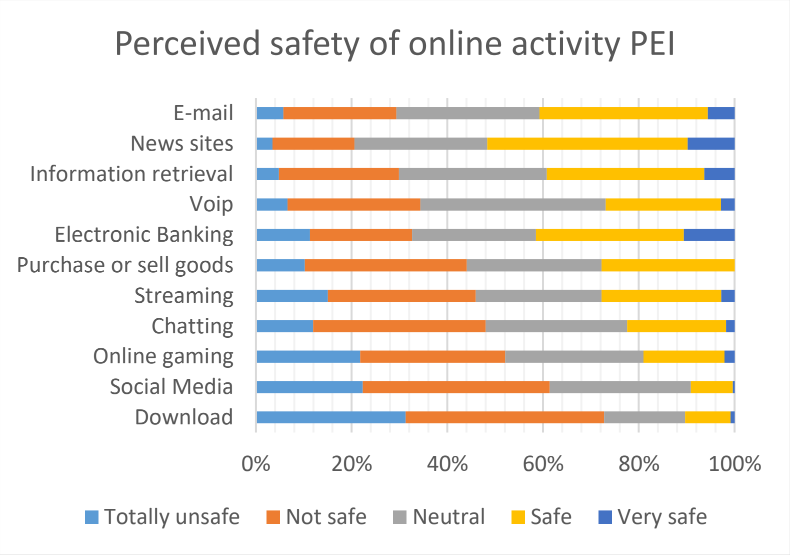


Table 27 PEI: Perceived safety of activity

The perceived safety of the different activities of the PEI's (see table 27) is rather low and comparable with the PDI's (see table 21). There is only one activity where more than half of the PEI's perceive the activity at least "safe", namely visiting news sites. For searching information online, emailing, electronic banking, VoIP, Buy & Sell goods online and streaming more than half of the PEI's perceive the activity less safe than "safe". For social network sites, online gaming, chatting and downloading this fraction even rises to more than 75%.

Security measures taken

4.8% of the PEI's don't use any of the security measures to protect themselves against any kind of cybercrime. On average, the PEI's protect themselves using 5.54 security measures (SD=2.15). Also here malware (M=4.56 SD=2.03) is the cybercrime from which they protect themselves the most, followed by hacking (M=3.92 SD=2.22), scams (M=2.84 SD=1.80) and monitoring (M=2.22 SD=1.93). Quite a lot of the PEI's are implementing adaptive social security measures with 73.5% checking the sender and content for anomalies and 88.8% being careful with third parties. A surprising high 15.5% of them decreases or stops certain online activities as a maladaptive security measure (see table 28). This is another indicator of opportunity costs. Just 38.1% of the sample pays for the software they use in contrast to 61.7% using free software. A quite high 71% tries to update their software and OS.

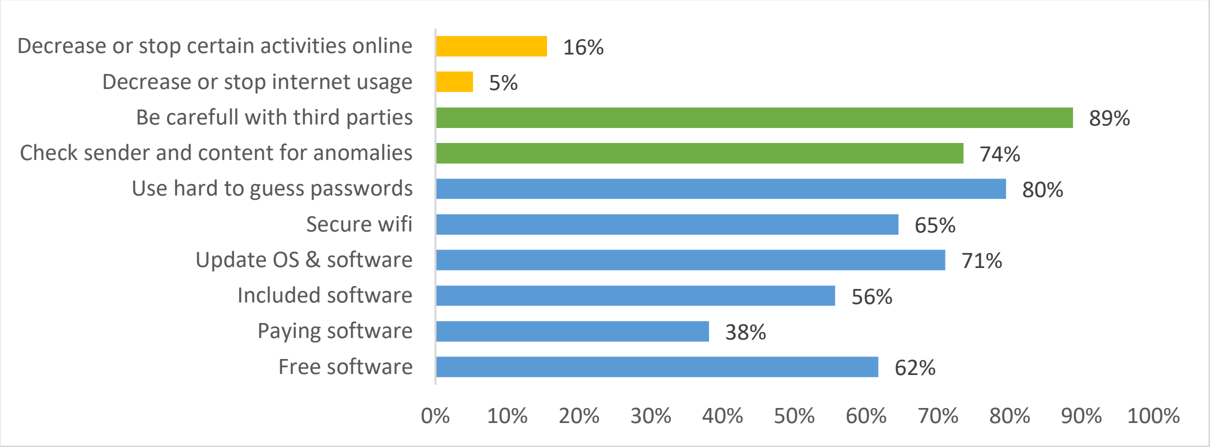


Table 28 PEI: Security measures taken

Victimisation rate PEI

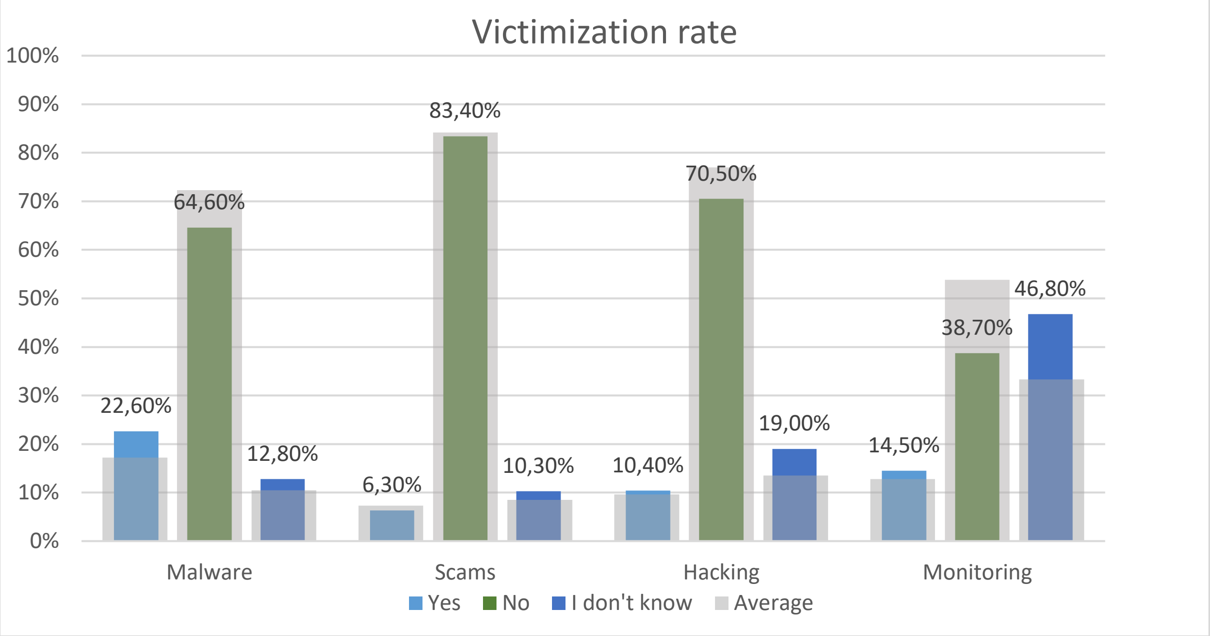


Table 29 PEI: Victimisation rate

63.7% of the PEI's state that they were never victimised by any of the cybercrimes or don't know of a victimisation event. Furthermore, it is mostly malware (22.60%) and monitoring (14.50%) PEI's were a victim of (see table 29). Moreover, there are more victimized PEI's from malware (p<.01) than expected (χ^2(8)=19.619, p<.05). Additionally, there is a high overrepresentation of PEI's saying they don't know if they were victimized by hacking (p<.001) (χ^2(8)=30.061, p<.001) or monitoring (p<.001) (χ^2(8)=47.766, p<.001).

There are more PEI's not knowing if they are victimized by hacking & monitoring than expected

4.2.5 Optimistic experienced internet user (OEI)

OEI - Passport

Demographics 17.0%

- Younger (M=42 SD=15.16)
    - More 18-34 (p<.001) & 35-44 (p<.05)
    - Less 65+ (p<.001) & 55-64 (p<.001)
- More jobless people
    - More students (p<.001) & people searching for job (p<.05)
    - Less (semi-)retired (p<.01)
- Higher education
    - More lowest Bachelor degree (p<.05)
- More from Brussels (p<.001)
- Less from Flanders (p<.05)

Internet diet

- Top tasks online
    - Information tasks
    - Social tasks
    - Electronic banking
- more often than the rest (p<.001)

Online perceived safety

- Internet is very safe

Internet diet & perceived safety of online activities

The OEI's are just like their pessimistic siblings mainly using the internet for traditional tasks like searching information, visiting news websites and emailing as more than 75% of them do this at least once a day. They are using social network sites even more with more than 75% using it every day. Electronic banking is done at least once a month by 75%. All the other activities are done at least monthly by half of the OEI's.

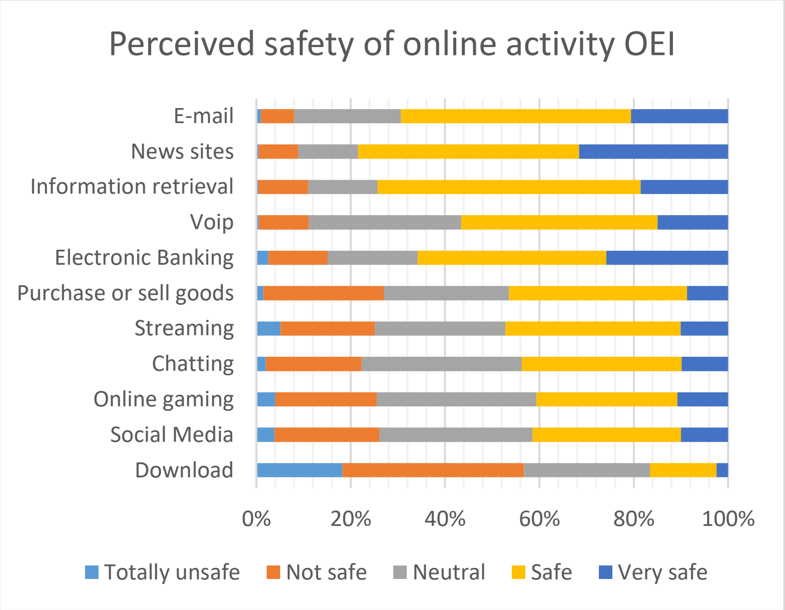


Table 30 OEI: Perceived safety of activity

The OEI's perceive activities in general as safe (see table 30), comparable with the ODI's (see table 18). More than 70% of the cluster perceive searching information, visiting news sites, and emailing as "safe" or safer. For electronic banking this fraction is still more than 60%. For online gaming, buy & sell goods online, Voip, chatting, social media and streaming this fraction is still more than 40%. Only for downloading this fraction drops to less than 20%.

Security measures taken

4.7% of the OEI's don't implement any of the security measures. On average they use 5.35 security measures (SD=2.19456). And just as in all other profiles they protect themselves the most against malware (M=4.32 SD=2.15783) followed by hacking (M=3.57 SD=2.27805), scams (M=2.7351 SD=1.98182) and monitoring (M=2.3406 SD= 2.24857). This Security behaviour is very much comparable to the pessimistic experienced internet user. There is no significant difference between the two groups if you compare the amount of security measures one takes against malware (t(463)= 1.291,p=.198), scams (t(463)= .585,p=.559), hacking (t(463)= 1.651,p=.100) or monitoring (t(463)= -.645,p=.519).

There is, however, a difference in which security measures they take, with the OEI's using significantly less maladaptive security measures. They decrease or stops certain activities less often than the pessimistic experienced internet user (p<.01)(χ^2(4)=78.310,p<.001) (see table 31). Just 7.7% of the OEI's decrease or stop certain activities online and just 4.1% of them decrease or stop using the internet as a whole.

With just 32.4%, the OEI's have the least percentage of people using paid software to secure themselves against cybercrime.

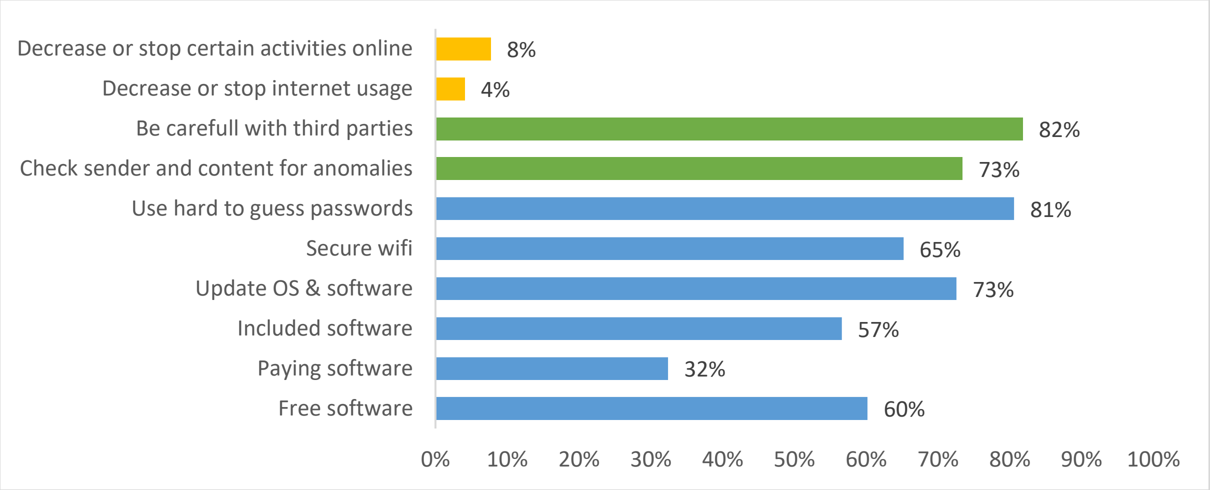


Table 31 OEI: Security measures taken

Victimisation rate OEI

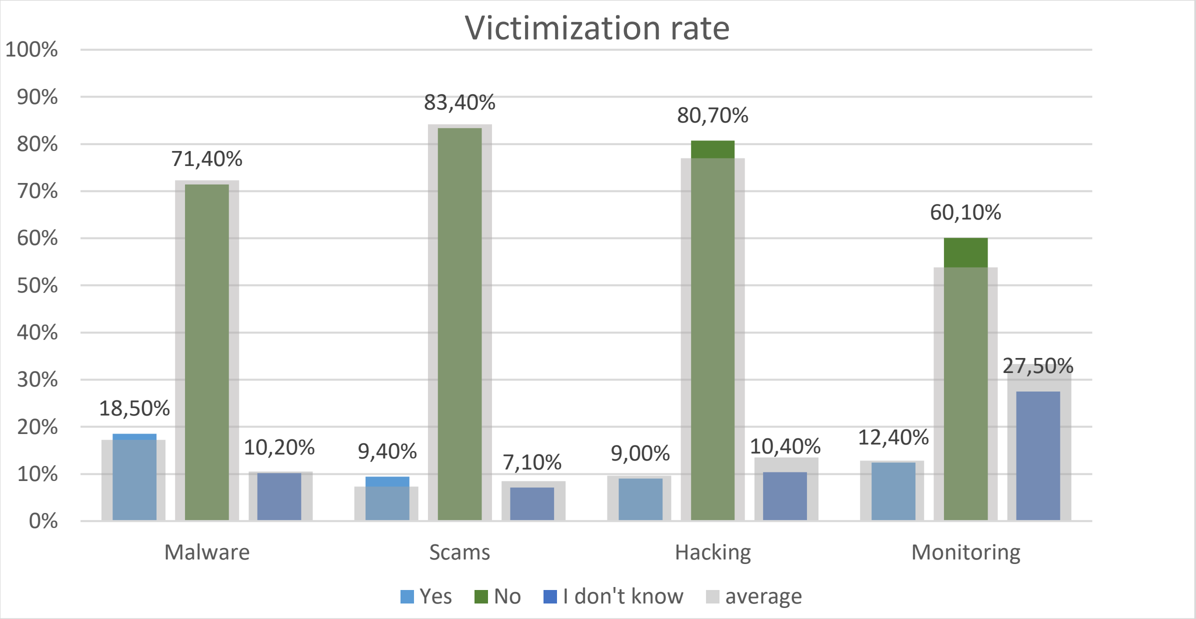


Table 32 OEI: Victimisation rate

Also in this cluster malware is the biggest threat (18.50%) followed by monitoring (12.40%), hacking (9.40%) and scams (9.00%).

In the cluster of OEI's, there is no over- or underrepresentation for the victimisation of any cybercrime except for monitoring where there is an overrepresentation of people not being victimized by monitoring (p<.05) (χ^2(8)=47.766, p<.001) (see table 32). This adds to the OEI's optimistic view.

4.2.6 Typologies, mutual comparison

Our typologies are per definition different in terms of internet usage, perceived security of the internet and security measures taken. It is however interesting to also compare these clusters in terms of victimisation rates and costs. Therefore in the following chapter, this comparison is done in addition to their defining variables.

Online activities

If we look at the online activities every cluster takes part in, we can clearly see a distinction between people using the internet mostly for traditional tasks such as retrieving information, sending emails or visiting news sites and people using the internet for more advanced tasks such as chatting, downloading and streaming.

If you look at the devices one uses to do these activities and the activities they perform, we can differentiate three distinct groups in the five clusters.

The ODI's and PDI's are generally having the same internet diet. They are mutually not significantly different on any of the measures of the activities. They score higher on every activity than the IUI's but lower than the PEI's and OEI's. Therefore we call the ODI's and PDI's intermediate internet users.

The IUI's know by far the least online activities

The PEI's and OEI's also have the same internet diet. They are scoring the highest on every single online activity but don't differ significantly from one another. We call these two clusters advanced internet users.

As a third group, we have the IUI's who uses the internet in a significantly different way than the other two groups of clusters. They score lowest on every online activity. We call this cluster the novice internet users.

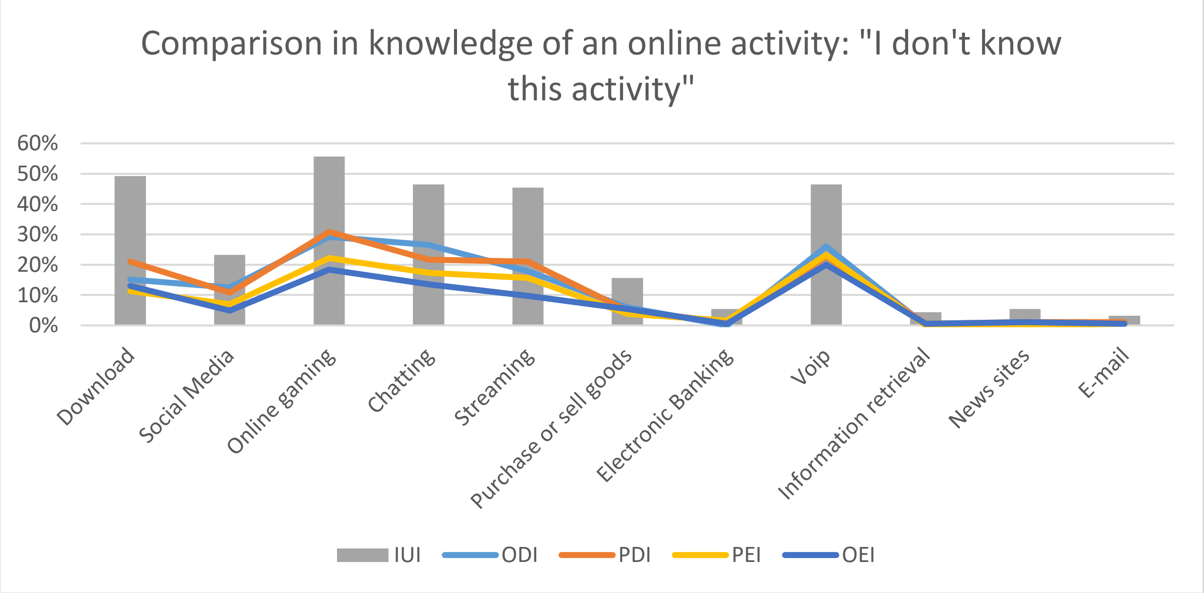


Table 33 Comparison of knowledge of online activities

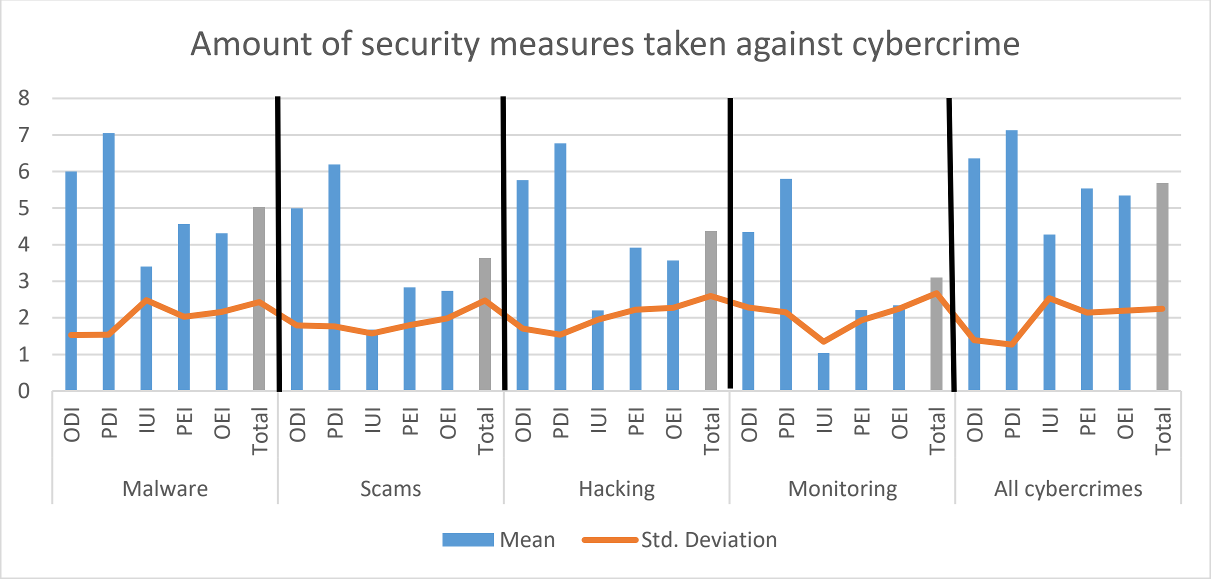
It is clear that the IUI's know all the activities much less than the other clusters (see table 33).

Security measures

We compared the security measures of the different clusters in terms of the amount of security measures but also in terms of which kinds of security measures a cluster uses.

Amount of security measures

If we look at the amount of security measures a cluster takes against certain cybercrimes we can conclude that the different cluster differ significantly from one another in the amount of security measures one takes against malware (F(4)=145.832, p<.001), scams(F(4)=303.377, p<.001), hacking(F(4)=245.260, p<.001), monitoring(F(4)=261.181, p<.001) and all of the cybercrimes combined (F(4)=83.794, p<.001).



	Malware						Scams						Hacking						Monitoring						All cybercrimes				
	ODI	PDI	IUI	PEI	OCEI	Total	ODI	PDI	IUI	PEI	OCEI	Total	ODI	PDI	IUI	PEI	OCEI	Total	ODI	PDI	IUI	PEI	OCEI	Total	ODI	PDI	IUI	PEI	OCEI
Mean	6,0	7,0	3,4	4,6	4,3	5,0	5,0	6,2	1,7	2,8	2,7	3,6	5,8	6,8	2,2	3,9	3,6	4,4	4,3	5,8	1,0	2,2	2,3	3,1	6,4	7,1	4,3	5,5	5,3

Table 34 Amount of security measure by cluster

Just as with their internet diet, the PEI's and the OEI's are taking approximately the same amount of security measures. There is no significant difference between the two for any of the cybercrimes (malware; p=.774, scams; p=.983, hacking; p=.460, monitoring; p=.977, all of them combined; p=.905). Compared to the other clusters they take significantly fewer security measures than the ODI's and the PDI's but significantly more than the IUI's.

The IUI's take the least security measures

All the other cluster differ significantly from one another in the amount of security measures they take against any cybercrime (p<.01 on every occasion). The PDI's implements generally the most security measures, followed by the ODI's. The cluster that takes the least security measures is the IUI's. This is true across all the cybercrimes.

Types of security measures

If we compare the different types of security measures a cluster takes, we see that the clusters are significantly different for technical adaptive security measures (F(4)=66.500, p<.001), social adaptive security measures (F(4)=43.070, p<.001) and maladaptive security measures(F(4)=22.160, p<.001).

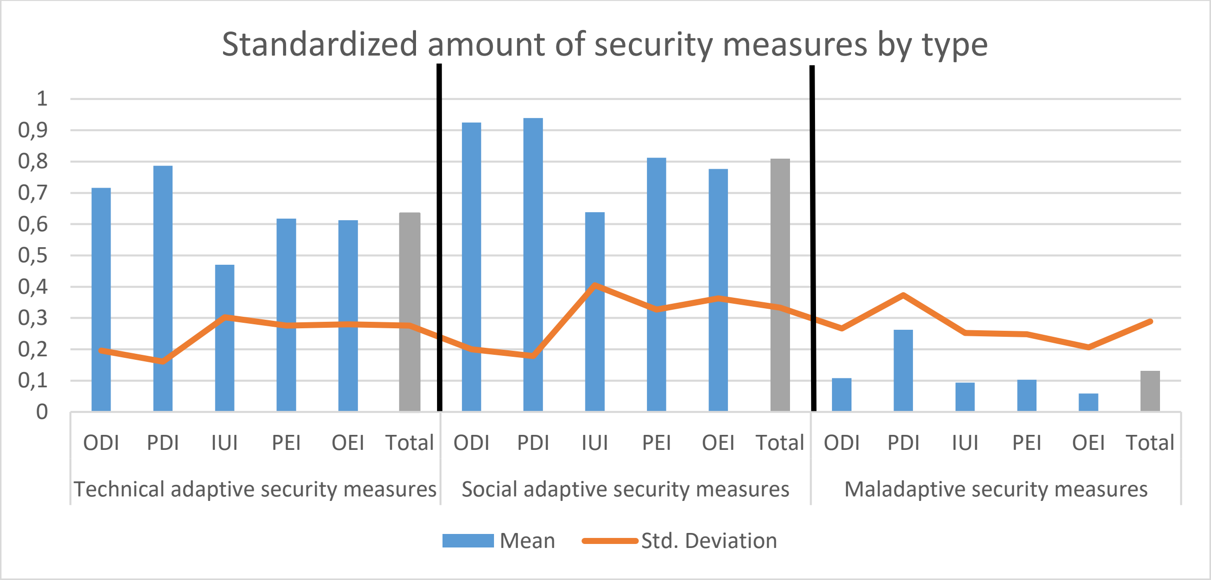


Table 35 Security measures by type by cluster

We can again make three groups, the ODI's and PDI's don't differ significantly in the technical (p=.061) and social adaptive security measures (p=.993). The PEI's and OEI's are also one group as they also don't differ significantly in the technical (p=1.000) and social adaptive security measures (p=.829).

The defensive internet users use most adaptive security measures, followed by the experienced internet users. The IUI's applies least technical and social adaptive security measures and does this significantly less than the others (p<.001 for both).

It is however interesting to look at the maladaptive internet users where only the PDI's differ significantly (p<.001) from the others, they apply the most maladaptive security measures. This could mean that the PDI's are trying to defend their self but don't really know how to. Therefore they just implement everything without thinking about the effectiveness.

The PDI's take most maladaptive security measures

Multiple uses of security measures

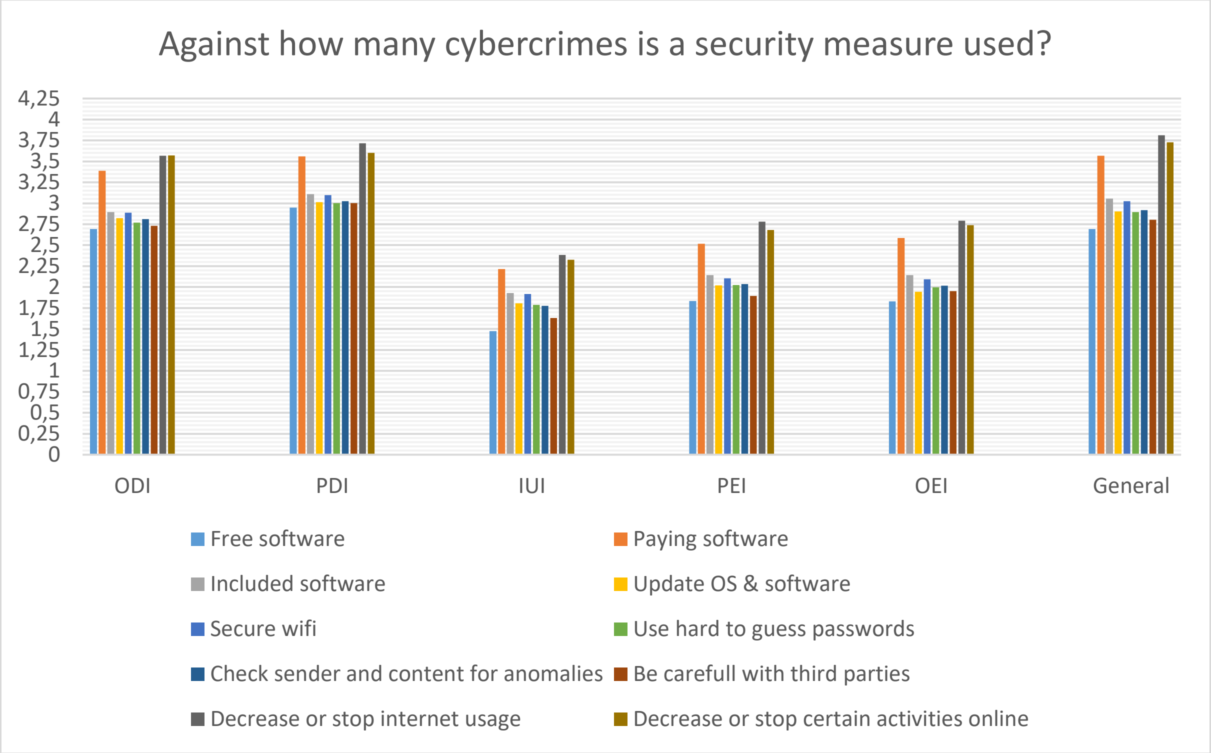


Table 36 Amount of cybercrimes one seeks protection for by cluster

If we look at the amount of crimes a certain security measure is used against we can see that if people used maladaptive security measures (such as decreasing or stopping internet usage or decreasing or stopping certain activities online) they do this to counter most cybercrimes.

Furthermore we see that there is a difference between the clusters for every security measure (free software (F(4)=53.376, p<.001), paying software (F(4)=34.689, p<.001), included software (F(4)= 29.228, p<.001), Update OS & software (F(4)=36.584, p<.001), Secure Wi-Fi (F(4)=32.449, p<.001), Hard password (F(4)=34.540, p<.001), check sender (F(4)=34.852, p<.001), be careful with third parties (F(4)=43.805, p<.001), decrease or stop internet (F(4)=37.348, p<.001) and decrease or stop activity (F(4)=34.507, p<.001)) .

There are two bigger groups to be distinguished. On one hand, we have the ODI's and PDI's who generally use every security measure (if they implement it) against most threats. And on the other hand, we have the IUI's, PEI's and OEI's who use every security measure (if they implement it) against fewer threats. The difference between these two groups are significant (p<.001 on every occasion), within the groups there is no significant difference. This measure can indicate how much a certain group trusts a security measure to protect themselves, for the optimistic and pessimistic defensive internet user this trust is thus higher.

The ODI's and PDI's implement each security measures against most threats

Victimisation rate

The victimisation rate between the different clusters differs significantly for malware (χ^2(8)=19.619, p<.05), hacking (χ^2(8)=30.061, p<.001) and monitoring (χ^2(8)=47.766, p<.001). For scams, this is however not the case (χ^2(8)=14.623, p=.067).

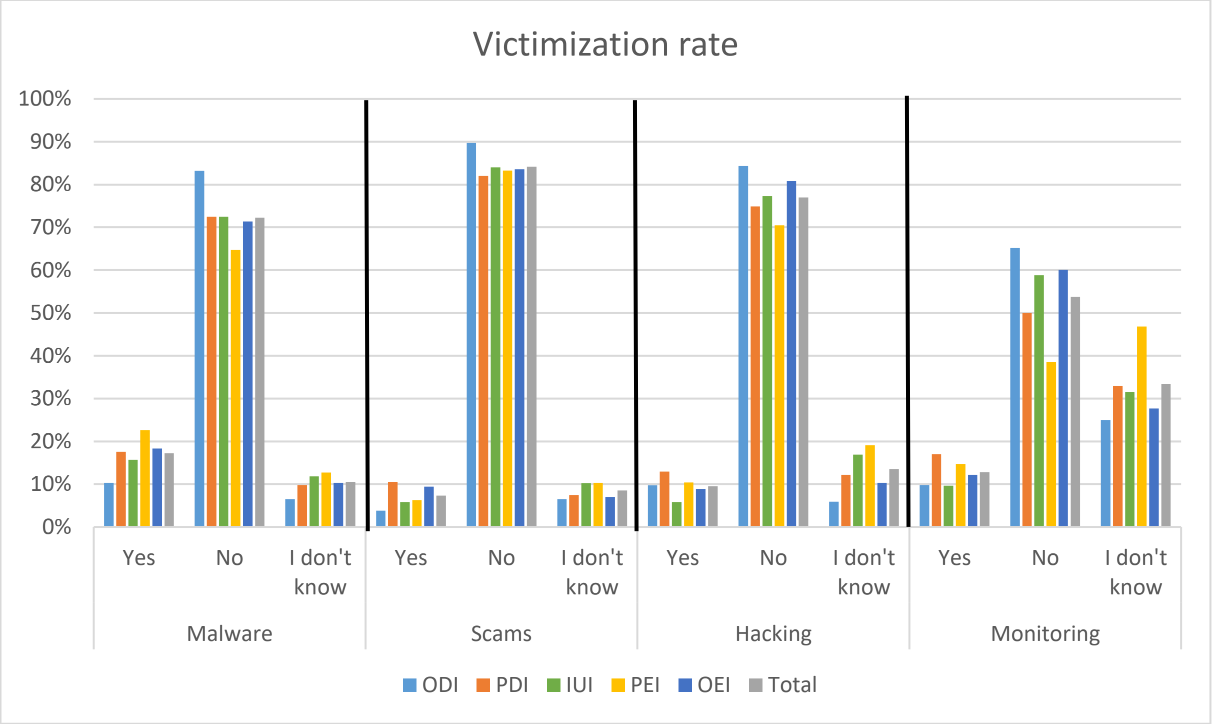


Table 37 Victimisation rate by cluster

Here we can see that significantly less (p<.01) ODI's and significantly more PEI's (p<.01) are victimized by malware than expected.

There are significantly more PDI's that are victimized by hacking (p<.01) and significantly less IUI's that are victimized by hacking (p<.01) than expected. Interestingly there are significantly more PEI's (p<.01) and more IUI's (p<.05) that state they don't know if they have been hacked than expected.

For monitoring, there is also a significant overrepresentation of the PDI's that state they were victimized by monitoring (p<.05) and a significant underrepresentation for IUI's stating they were victimized by monitoring (p<.05).

Furthermore, there is a very significant overrepresentation of PEI's that don't know if they are victimized by monitoring (p<.001) and an underrepresentation of the ODI's that don't know if they are victimized by monitoring (p<.001).

We can thus conclude that in general the PDI's are despite their defensive character being victimized the most. Also, the PEI's are being victimized more often than expected especially by malware. The ODI's are being victimized the least, especially by malware.

> *PDI's are despite their defensive character being victimized the most*

Surprisingly the IUI's are less than expected victim of monitoring or hacking. This could be because they don't notice if they are victimized or that they don't or to a lesser extent than the rest do the activities online in which one could get hacked, such as using social network sites.

Security measures combined with victimisation rate

Looking at the security measures and the victimisation rate it is interesting to notice that the amount of protection someone takes is not connected to their victimization. The PDI's are despite implementing the most security measures against scams, hacking or monitoring also being victimized the most by these cybercrimes. PDI's, however, also implement most maladaptive security measures, which do not protect them against cybercrime.

The IUI's are despite implementing by far the least security measures against the different cybercrimes not most victimized, they are even least victimized for monitoring and hacking.

Also, experience is not the differentiating variable to whether or not being victimized by cybercrime. The PEI's are being victimized by malware most of all clusters. The OEI's, however, are much less victimized than its pessimistic cousin.

Cybercrime cost

Direct costs

For this data, only the victimized people are taken into account. As these are just a small fraction of the population (see table 38), the conclusions in this section are solely of exploratory nature.

Amount of …	Malware victims		Scams victims		Hacking victims		Monitoring victims	
ODI	19	10.27%	7	3.78%	18	9.73%	18	9.73%
PDI	52	17.63%	31	10.51%	38	12.88%	50	16.95%
IUI	49	15.65%	18	5.75%	18	5.75%	30	9.58%
PEI	57	22.62%	16	6.35%	26	10.32%	37	14.68%
OEI	39	18.31%	20	9.39%	19	8.92%	26	12.21%

Table 38 Amount of victims by cybercrime by cluster

Direct monetary costs

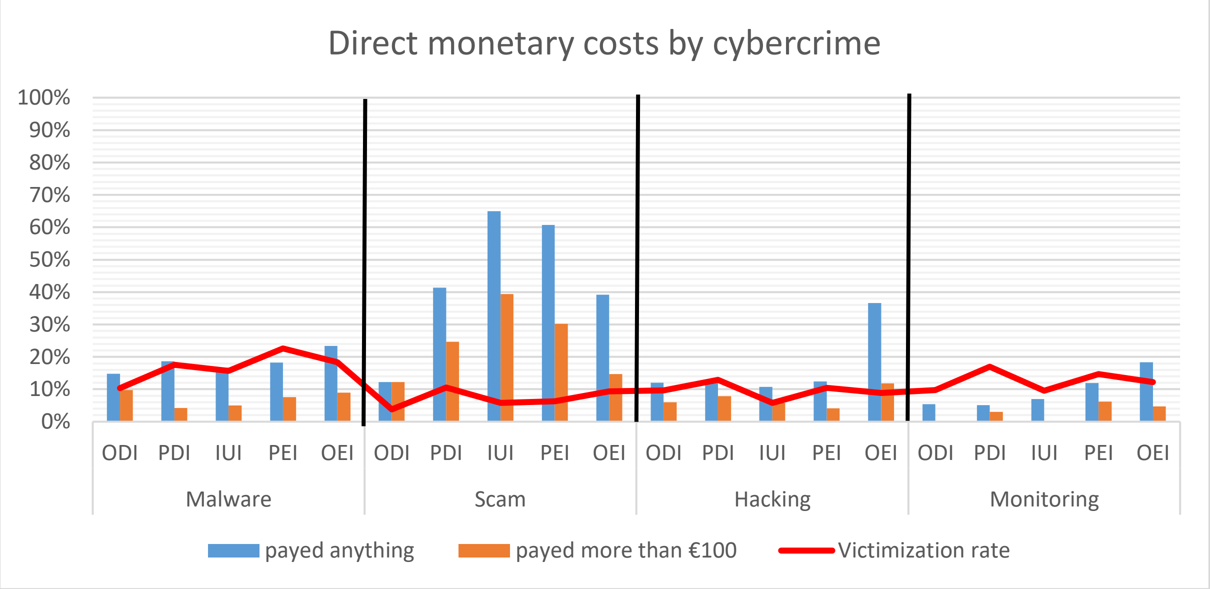


Table 39 Direct monetary cost by crime by cluster

More than 80 % of the ODI victims paid no direct costs for any of the cybercrimes (see table 39). This is also true for the PDI victims, IUI victims and PEI victims for all cybercrimes but scams. Moreover, scams are in general most expensive for all clusters but ODI victims. For all cybercrimes except for scams the OEI victims suffer the highest direct monetary costs. For scams this is the IUI victims, a staggering 65% of the IUI victims state that they paid direct costs as a consequence of scams.

> *65% of the IUI's state they paid money as a direct consequence of scams*

Interestingly, however, is that the victimisation rate is not linked to the amount of people stating that they suffered direct costs (see table 39). So even if they are victimized less often this does not mean they have less direct monetary costs for when they are victimized.

For a detailed overview tables of all direct monetary costs per cybercrime per cluster see Appendix E

Direct non-monetary costs

As there are no 30 people in every cluster for every cybercrime the central limit theorem couldn't be applied. The remaining respondents are also not normally distributed. A Kruskal-Wallis test show that there is no significant difference between the clusters for the sumscale of harm experienced by malware(H(4)=2.260, p=.688), scams(H(4)=4.357, p=.360), hacking(H(4)=1.491, p=.828) or monitoring(H(4)=7.219, p=.125).

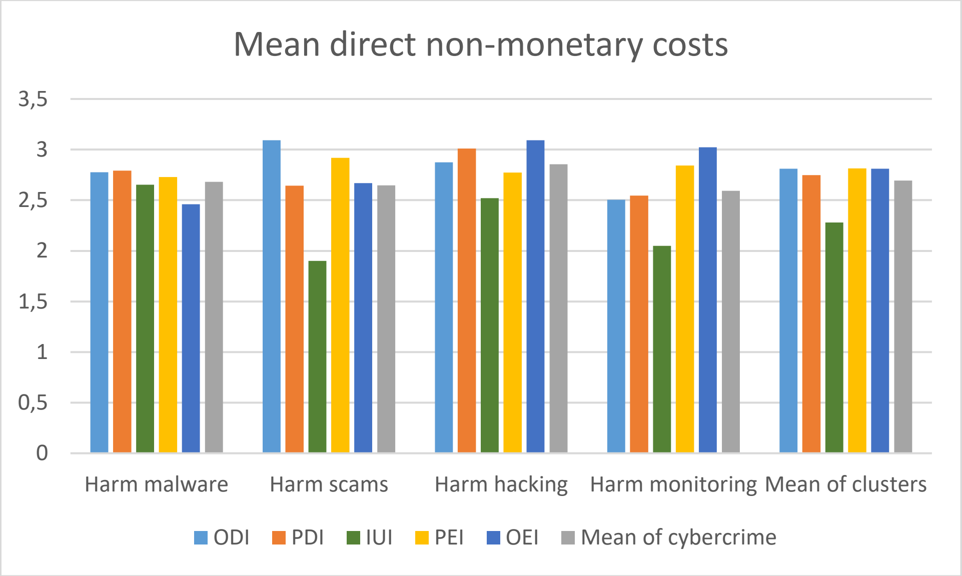


Table 40 Mean direct non-monetary cost by crime by cluster

With '3' being moderately harmful we see that no matter the crime all crimes are seen on average about moderately harmful.

If we then look at the direct non-monetary direct costs in more detail. We see that after more Kruskal-wallis tests for every cybercrime for daily activities (malware H(4)=.819, p=.936; scams H(4)=1.948, p=.745; hacking H(4)=1.331, p=.856; monitoring H(4)=4.530, p=.339), reputation (malware H(4)=.1.805, p=.772; scams H(4)=5.024, p=.285; hacking H(4)=1.295, p=.862; monitoring H(4)=4.996, p=.288) and privacy (malware H(4)=3.547, p=.471; scams H(4)=3.771, p=.438; hacking H(4)=.980, p=.913; monitoring H(4)=8.760, p=.067) there is no significant difference to be found between the different clusters. For a general overview of the non-monetary direct costs see table 16.

Opportunity costs

Opportunity costs are measures with direct questions, the maladaptive security measures and the correlation between perceived safety and frequency of use of an online activity.

Opportunity costs (direct questions)

If we look at these opportunity costs in detail we see that 10.7% of the PDI's say they agree or totally agree with the statement they reduce their electronic banking because of cybercrime. This is by far the most with just 3.9% for the OEI's, 5.8% for the IUI's, 8.4% for the PEI's and 2.3% for the OEI's. For online shopping again 13.6% of the PDI's agree or totally agree, for IUI this is an equally high 13.9%. The rest scores with 6.2% (OEI's), 4.1% (PEI's) and 4% (OEI's) considerably lower. An even higher 16.6% of the PDI's agree or totally agree for social networks. This is again much higher than all the other clusters (IUI's= 7.5%, ODI's=3.6%, PEI's=9.5% and OEI's= 2.4%). If we base ourselves on these findings we can claim that the PDI's and to some extent the IUI's experience the most opportunity costs. This is still true if we analyse the sumscale (α=.832). The different clusters differ significantly from each other in terms of opportunity costs if we look at the sumscale of the three questions (F(4)=15.051, p<.001)

The PDI's and IUI's experience the highest opportunity costs

The PDI's (M=2.1402 SD=.92510) and the IUI's (M=2.1092 SD=.86670) score highest and don't differ significantly from one another (p=.997).

Then you have the PEI's (M=1.8596 SD=.78160) and the OEI's (M=1.7933 SD=.77354) who don't differ significantly from one another (p=.970).

The ODI's don't differ significantly from the OEI (M=1.5930 SD=.72006) either (p=.319).

If we look at the different means of the clusters we can, however, determine that in general the perceived opportunity costs on electronic banking, social network sites and buying and selling goods online is not high. The average response is lower than neutral (3) in the statements about opportunity costs. There is, however, a significant fraction for which these opportunity costs are considerable, especially for the PDI's with 22.3% of them scoring more than neutral (3) and 18.2% of the IUI's scoring more than neutral (3) for the sumscale of the direct questions on opportunity costs.

Maladaptive security measures

The PDI's implement by far the most maladaptive security measures with 26.26% reducing or stopping internet usage or a specific online activity as security measures (cfr. supra). All the other clusters don't differ significantly from another. This does however not mean they do not implement maladaptive security measures with on average 10.7% of the ODI's, 9.32% of the IUI's, 10.33% of the PEI's and 5.9% of the OEI's reducing or stopping internet usage in general or a specific online activity as security measure (for more detailed information about these security measures see table 19, 22, 25, 28 & 31).

Correlation between perceived security and frequency of an online activity

For all clusters but for the OEI's, there are more than six significant correlations to be found that indicate that the more someone perceives an activity as safe, the more they will perform that activity (see table 41). Surprising these correlations are higher for activities that are not or to a lesser extent done by the cluster. These correlations are quite high and numerous for all but the OEI's.

Table 41 Correlations between perceived safety and frequency of use of online activities per cluster

		Searching information	Visiting News websites	E-mail	Electronic banking	Online Gaming	Social Network Sites	Chatting	VoIP	Buy/sell goods online	Download	Stream
ODI	r	-.026	.036	.054	.049	.448**	.228**	.356**	.409**	.295**	.119	.332**
	p	.725	.628	.468	.508	<.001	<.001	<.001	<.001	<.001	.139	<.001
PDI	r	.07	.158**	.082	.144*	.347**	.303**	.376**	.297**	.265**	.069	.332**
	p	.235	<.01	.164	.014	<.001	<.001	<.001	<.001	<.001	.273	<.001
IUI	r	.095	.140*	.169**	.211*	.323**	.265**	.174**	.301**	.317**	.097	.272**
	p	.098	<.05	.<.01	<.001	<.001	<.001	<.001	<.001	<.001	.149	<.001
PEI	r	.163**	.150*	.09	.049	.327**	.288**	.263**	.219**	.158*	.115	.294**
	p	<.01	<.05	.155	.446	<.001	<.001	<.001	<.001	<.05	.083	<.001
OEI	r	.058	.027	-.132	.008	.14	.103	.271**	.135	-.009	-.067	.150*
	p	.397	.695	.053	.907	.061	.139	<.01	.071	.899	.354	.035

If we look at the average correlation of these items we see that these are much higher for the ODI's than for the rest (see table 42).

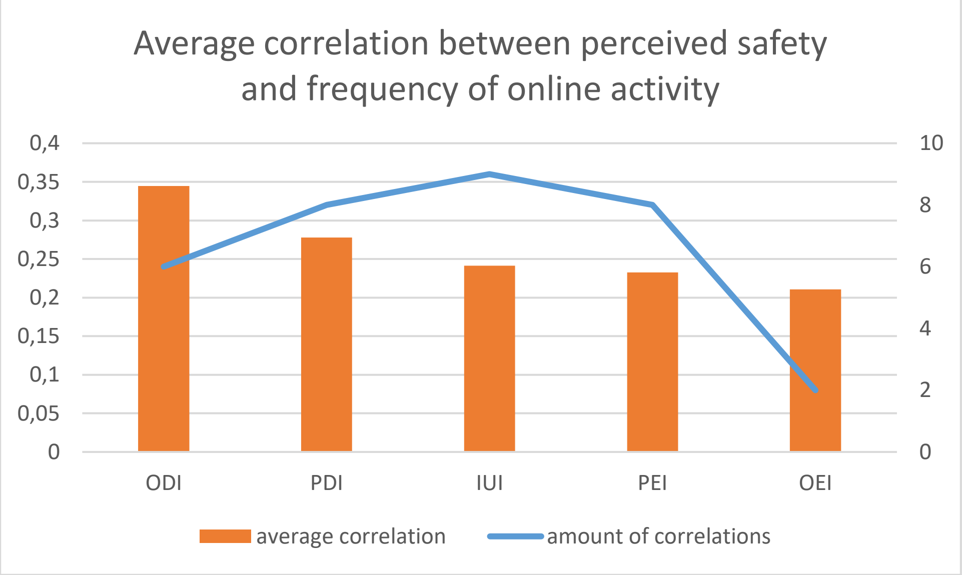


Table 42 Average correlation between frequency and perceived security of an online activity by cluster

It is important to note that the six significant correlations that were found with the optimistic defensive internet users are to be found in all the other cluster (except for the optimistic experienced internet user). These activities are:

- Online gaming
- Using social network sites
- Chatting
- Calling over the internet
- Buying and selling goods online
- Streaming

This means that for four of the five clusters these activities incorporate opportunities they lost to some extent.

Conclusion

All but the OEI's experience opportunity costs to some extent

Four of the five cluster experience in one way or another opportunity costs because of cybercrime. This is visible in the direct questions about opportunity costs, the maladaptive security measures they take but also in the correlation between the perceived security of an activity and the frequency of doing a certain activity online.

For every measure of opportunity costs the OEI's show that they perceive the least opportunity costs of all the clusters.

Defence costs

There is no normal distribution as there are less than 30 respondents who answered the defence cost with not "€0" in for at least one cluster in every cybercrime. The remaining respondents are not normally distributed either, therefore we performed a Mann-Whitney.

There is no significant difference in terms of defence costs in between clusters

This test shows us that none of the defence costs against any type of cybercrime differs significantly between the clusters. This is true for defence costs against malware (H(4)=6.199 p=.185), scams (H(4)=6.200 p=.185), hacking (H(4)=4.882 p=.300) and monitoring (H(4)=1.903 p=.754).

For cybercrime in general, however, we can apply the central limit theorem as all of the clusters have at least 30 respondents that answered something else than €0. After a one-way Anova analysis, however, also here there is no significant difference between the clusters (F(4)=1.544 p=.190).

For the general information about the defence costs on the whole sample see table 17.

Awareness of cybercrime and security measures

A one-way Anova shows us that there is a significant difference between the clusters in terms of the sumscale (α=.839) of awareness of the cybercrimes (F(4)=88.218 p<.001) and the sumscale (α=.882) of the awareness of the security measures (F(4)=69.130 p<.001). A post-hoc Sheffe test shows us that the IUI's score significantly (p<.001) lower (M=2.9104 SD=1.06673) on the awareness of cybercrimes than the ODI's (M=3.4013 SD=.92579), PDI's (M=3.5568 SD=.84757), PEI's (M=3.5256 SD=.94314) or the OEI's (M=3.3629 SD=.97473). Furthermore, the IUI (M=3.1338 SD=.79863) also score significantly lower on the awareness of security measures (p<.001) than the ODI's (M=3.7435 SD=.63426), PDI's (M=3.7122 SD=.70187), PEI's (M=3.4688 SD=.75300) or the OEI's (M=3.5077 SD=.65728). These results lend to support that the IUI is not really victimized less but is unaware if they are victimized.

The IUI was by far least aware of the different cybercrimes and security measures

Conclusion typologies, mutual comparison

Using a cluster analysis we differentiated between five typologies. The optimistic defensive internet users (ODI), the pessimistic defensive internet users (PDI), the inexperienced unknowing internet users (IUI), the pessimistic experienced internet users (PEI) and the optimistic experienced internet users (OEI).

The IUI's have a low frequency of internet use and mainly engage in traditional online activities, they are seen as the novice internet users. ODI's and the PDIs can be considered the intermediate Internet users. They use the Internet more often than the novice users but less often than the advanced internet users. They use the internet for mainly the same activities as the IUI's. The PEI's and the OEI's are the biggest and most advanced internet users.

Taking into account the security measures of the groups we notice that the advanced internet users (= PEI's & OEI's) implement a similar amount of security measures. The intermediate internet users (=ODI's & PDI's), however, do not. They are significantly different from one another when it comes to maladaptive security measures, with the PDI's implementing significantly more maladaptive security measures than the ODI's.

The PDI's implement significantly more maladaptive security measures than all the rest

The PDI's implement significantly more maladaptive security measures than all the other typologies. This could mean that they are not able to protect themselves in a good way. The ODI's and PDI's, however, don't differ significantly on their adaptive security behaviour. They implement in general more security measures than the advanced internet users, who in their turn implement more security measures than the IUI's.

The victimisation rates are higher than expected for the PEI's for malware. The IUI's are victimized less than expected by hacking or monitoring. This could be explained by their lack of awareness of cyberthreats and security measures. The ODI's are also victimized less than expected for all cybercrimes but scams. For the PDI's, the victimisation rate is higher than expected for hacking and monitoring. For scams, they also have the highest victimisation rate although not significantly more than expected. This adds to the presumption that they are not able to adequately protect themselves.

The IUI lack awareness to notice if they are victimized

The IUI are paying most money as a consequence of scams

In general, monitoring is seen as the least expensive cybercrime and scams as the most expensive cybercrime. The IUI's are paying the most money as a consequence of scams. Interestingly, the victimisation rate is not linked to the amount someone pays as a direct consequence of a cybercrime.

Opportunity costs are felt by every cluster but the OEI's. We can conclude that the PDI's & IUI's are experiencing the most opportunity costs. The PDI's implements most maladaptive security measures and scores together with the IUI's the highest on the direct opportunity questions.

As for non-monetary direct costs or defence costs, there is no significant difference between the clusters.

The ODI's are also experiencing opportunity costs as they have the highest average correlation between the perceived security and the frequency of use of a certain online activity. The PEI's also experience opportunity costs but to a lesser extent.

Opportunity costs are felt by all clusters but the OEI's

If we look at the victimisation rate and combine this with the security measures we can conclude that there are two clusters that are of special interest for risk communication. First, we argue that the IUI's are an important cluster for risk communication because they lack awareness and are not fully able to know if they are victimized or not. They are not protecting themselves against cybercrime when compared to more experienced internet users, and are still experiencing the highest direct costs from scams.

The PDI's and the IUI's are important clusters for risk communication

The PDI is implementing all security measures it can, maladaptive or adaptive and has a general distrust on the Internet. Just like the IUI, this cluster stays an important cluster for risk communication because they are not fully able to effectively and adequately protect themselves against cybercrime. In addition, they also suffer many opportunity costs when trying to protect themselves.

4.3 Population evolution 2015 - 2017

4.3.1 Trust & perceived security

Comparing the trust levels of the internet between 2015 and 2017 we find a significant yet small difference where people nowadays (M=2.60 SD=.7605) are less concerned about the internet in general than in 2015 (M=2.73 SD=.2219) (t(2418)=-4.318, p<.001).

In 2017 online banking and chatting is considered safer than in 2015

No difference was found in the perceived safety of online activities between 2015 and 2017 for information retrieval (p=.151), visiting news sites (p=.965), sending emails (p=.165), visiting social media (p=.627), using VOIP (p=.179), selling or buying things online (p=.967) or downloading (p=.225). There is, however, a significant difference for online banking (p<.01) and chatting (p<.05). In the second wave, people seem to have higher levels of trust for these activities. The opposite was found for online gaming (p<.01) and streaming (p<.01). In 2015 people put more trust into the latter activities.

In 2015 streaming and online gaming was considered safer than in 2017

4.3.2 Victimisation rate

In 2015 40.4% were victimized by malware, in 2017 this is significantly less with 17.3% (p<.001). For monitoring, similar results were found, in 2015 24.8% and in 2017 12.9% of the people were victimized by monitoring (p<.001). For scams and hacking, no significant differences were found between 2015 and 2017.

4.3.3 Security measures[4]

On average significantly more technical adaptive security measures were employed in 2017: 63.5% of the offered technical adaptive security measures were used in 2017 as opposed to only 43.6% in 2015 (p<.001).

In 2017 significantly more adaptive and less maladaptive security measures were implemented than in 2015

For maladaptive security measures, the opposite is true. In 2015 66.9% of the people implemented at least one maladaptive security measure compared to only 19.2% in 2017.

4.3.4 Direct monetary cost

There is a significant difference between 2015 and 2017 for the direct costs of malware (U=45708.000, p<.001), scams (U=4109.500, p<.05), hacking (U=5036.500, p<.001) and monitoring (U=11654.500, p<.001). In 2015 higher costs were mentioned for these cybercrimes (see table 43-47).

	Malware					
	Frequency 2015	**Relative percentage of victims 2015**	**Total percentage 2015**	**Frequency 2017**	**Relative percentage of victims 2017**	**Total percentage 2017**
€0	174	49,7%	16,8%	162	81,5%	12,9%
<€20	36	10,3%	3,5%	9	4,7%	0,7%
€21-€200	115	32,9%	11,1%	21	10,7%	1,7%
€201-€2001	17	4,9%	1,7%	3	1,5%	0,2%
€2000+	8	2,3%	0,8%	3	1,5%	0,2%

Table 43 Comparison 2015/2017 direct monetary costs malware

	Scams					
	Frequency 2015	**Relative percentage of victims 2015**	**Total percentage 2015**	**Frequency 2017**	**Relative percentage of victims 2017**	**Total percentage 2017**
€0	18	30,0%	1,7%	48	53,7%	3,8%
<€20	11	18,3%	1,1%	2	2,1%	0,1%
€21-€200	14	23,3%	1,4%	23	25,2%	1,8%
€201-€2001	10	16,7%	1,0%	10	11,0%	0,8%
€2000+	7	11,7%	0,7%	7	7,9%	0,6%

Table 44 Comparison 2015/2017 direct monetary costs scams

[4] Not all analysis could be replicated with the data from 2015 as there were differences in the survey's. Social adaptive security measures were not included in the 2015 survey.

	Hacking					
	Frequency 2015	**Relative percentage of victims 2015**	**Total percentage 2015**	**Frequency 2017**	**Relative percentage of victims 2017**	**Total percentage 2017**
€0	31	48,4%	3,0%	93	84,0%	7,4%
<€20	5	7,8%	0,5%	7	5,9%	0,5%
€21-€200	15	23,4%	1,5%	6	5,6%	0,5%
€201-€2001	6	9,4%	0,6%	4	3,6%	0,3%
€2000+	7	10,9%	0,7%	1	0,9%	0,1%

Table 45 Comparison 2015/2017 direct monetary costs hacking

	Monitoring					
	Frequency 2015	**Relative percentage of victims 2015**	**Total percentage 2015**	**Frequency 2017**	**Relative percentage of victims 2017**	**Total percentage 2017**
€0	119	79,9%	11,5%	131	91,0%	10,4%
<€20	9	6,0%	0,9%	3	0,2%	0,2%
€21-€200	12	8,1%	1,2%	7	0,5%	0,5%
€201-€2001	5	3,4%	0,5%	1	0,1%	0,1%
€2000+	4	2,7%	0,4%	2	0,2%	0,2%

Table 46 Comparison 2015/2017 direct monetary costs monitoring

	Malware	**Scams**	**Hacking**	**Monitoring**
Median 2015	1.5	3	2	1
Median 2017	1	1	1	1

Table 47 Comparison 2015/2017 median of direct monetary cost by cybercrime 1=€0, 2=<€20, 3=<€200

4.3.5 Conclusion how has the population evolved between 2015 and 2017

People in 2015 trusted the internet significantly less than in 2017. The reduced victimisation rate of malware and monitoring combined with the increase of technical adaptive security measures makes us believe that people in 2017 are better armed against those cybercrimes. The victimization rate of scams and hacking, however, has not changed significantly, despite the increasing implementation of technical adaptive security measures.

In 2017 significantly less people were victimized by malware and monitoring

That said, the direct monetary costs have declined when we compare the direct monetary costs between 2015 and 2017. A plausible explanation may be that the concept of cost was differently operationalized in 2015 than in 2017. In 2015 cost was operationalised by only one single question that contained all costs linked to cybercrime.

4.4 Typology evolution 2015 - 2017 (RQ2.2)

The cluster analysis differentiated between 4 typologies in 2015 and 5 typologies in 2017. Although the groups are inherently different, to some extent, they do have similarities which allow us to compare the data between 2015 and 2017. For example, the inexperienced internet user (2015) is comparable to the inexperienced unknowing internet user (2017) (see table 48).

2015	**2017**
The conscious internet users (32.0%)	➔ The pessimistic experienced internet users (20.0%) ➔ The optimistic experienced internet users (17.0%)
The inexperienced internet users (35.3%)	➔ The inexperienced unknowing internet users (24.9%)
The resolved internet users (19.1%)	➔ The pessimistic defensive internet users (23.4%) ➔ The optimistic defensive internet users (14.7%)
The overly confident internet users (13.5%)	➔ All clusters but the IUI's

Table 48 Typology 2015/2017

4.4.1 General

Comparing the data between 2015 and 2017 we see that the inexperienced internet users are comparable to the inexperienced unknowing internet users. They are using the internet least often and for traditional purposes. Furthermore, they barely use security measures to protect themselves. This group is reduced from 35.3% to 24.9% in between 2015 and 2017.

The conscious internet user of 2015 is comparable to the pessimistic and optimistic experienced internet users of 2017. They are the internet users who use the internet most often, with most devices and with the highest variety. In general, these groups are younger and they implement quite a lot of security measures to protect themselves. The conscious internet users of 2015 had doubts about the safety of the internet which they perceive as not entirely safe. In 2017 this is divided between the PEI's who also doubt the safety of the internet and the OEI's who don't. The conscious internet users were in 2015 the second biggest group with 32.0%. The pessimistic (20.0%) and optimistic experienced internet users (17.0%) together account for about the same fraction with 37.0%.

The resolved internet users of 2015 show similarities to the 2017 defensive internet users, both the optimistic and pessimistic defensive internet users. The resolved internet user and the defensive internet users both implement a lot of security measures and have a moderate variety and frequency of internet use. The perceived safety of the internet is in 2017 (just like with the conscious internet users) divided between the pessimistic and optimistic defensive internet user. In 2015 the resolved internet users consisted of 19.1% of the sample, in 2017 this is much more with a combined 38.1% (PDI's = 23.4%, ODI's= 14.7%).

The overly confident internet user, however, is not that easily traceable. If we look at their internet use, we can compare them with the defensive internet users (both the optimistic and pessimistic). If we look at their perceived safety of the internet, we see they compare well to the optimistic defensive internet user or the optimistic experienced internet user. This comparison doesn't hold up when looking at the security measures taken. The amount of security measures the overly confident internet user takes can be compared to the optimistic or pessimistic experienced internet users' amount of security measures. This, however, doesn't hold true for the amount of cybercrimes they protect themselves against or for the older demographics of the overly confident internet user. It seems fair to say that the overly confident user has bits of every cluster but the inexperienced unknowing internet user in 2017[5]. Their 13.5% is thus divided over all the groups in 2017.

4.4.2 Security measures

Inexperienced internet user °2015 – Inexperienced unknowing internet user °2017

If we compare the inexperienced internet user between 2015 and 2017 we can see that in 2015 more maladaptive security measures were performed, with 32.6% reducing their internet activities and 57.6% reducing various activities online. In 2017, however, such counterproductive measures are less implemented, with only 7.4% decreasing or stopping internet usage and 11.3% decreasing or stopping a certain activity online .

Considering the adaptive security measures, the inexperienced unknowing internet user is scoring the lowest of all clusters of 2017(cfr. supra). In 2015 they implemented second to least adaptive security measures across the line (with the overly confident internet user implementing even fewer security measures). The inexperienced internet user has thus certainly not changed their adaptive security behaviour for the better.

Conscious internet user °2015 – Pessimistic/optimistic experienced internet user °2017

Looking at the maladaptive security measures of the pessimistic and optimistic experienced internet users in 2017, they rarely implement maladaptive security measures. This is in contrast to the conscious internet users in 2015, who scored much higher than the resolved internet users on the two maladaptive security measures; with 20.5% of them reducing their internet usage and 66.2% reducing certain activities online.

For the adaptive security measures, however, the conscious internet user also scored higher than the rest in 2015 with. They had "by far most security measures in place", thus Verdegem et al. (2015). In 2017 they are generally second in rank, but still implement quite a lot of adaptive security measures when looking at the different groups of clusters (cfr. supra).

The PEI's and OEI's in 2017 have thus changed their security behaviour with less maladaptive but also less technological security measures compared to 2015.

Resolved internet user °2015 – Pessimistic/optimistic defensive internet user °2017

11.1% of the resolved internet user reduced or stopped their internet usage as a security measure, 32.9% of them reduced or stopped a certain activity online. Doing so they implemented an average amount of maladaptive security measures compared to the other clusters of 2015. In 2017 the pessimistic and optimistic defensive internet user differ significantly on maladaptive security measures. The pessimistic defensive internet user implements by far the most maladaptive security measures (19.9% reducing or stopping internet usage, 32.7% reducing or stopping certain activities online) while the optimistic defensive internet user doesn't differ differently from the rest. They implement less maladaptive security measures than the pessimistic defensive internet users (10.2% reducing or stopping internet usage, 11.4% reducing or stopping certain activities online).

If we look at the adaptive security measures, the resolved internet users in 2015 are scoring average in percentage but are having 97.6% of them paying for software to protect against cybercrime. In 2017

[5] Because there is no clear comparable cluster found in 2017 for the overly confident internet user, there is no comparing analysis done.

the pessimistic and optimistic defensive internet users can be seen as a group and are implementing the most adaptive security measures of all clusters.

The PDI's are implementing more maladaptive and more technological adaptive security measures relative to the other clusters in 2017 compared to 2015. The ODI's however only implement more technological adaptive security measures

4.4.3 Victimisation rate

Inexperienced internet user °2015 – Inexperienced unknowing internet user °2017

If we compare the victimisation rate of the inexperienced internet users in 2015 and 2017 we can see a significant difference in self-reported victimisation rate, with the inexperienced internet users in 2015 having a higher victimisation rate than those of 2017 in all cybercrimes but hacking (see table 49).

Cybercrime	**Victimisation percentage 2015**	**Victimisation percentage 2017**	**Significance difference 2015 & 2017**
	Inexperienced internet user	IUI's	
Malware	38.3%	15.5%	<.001
Scams	10.4%	5.9%	<.05
Hacking	7.8%	5.9%	NS
Monitoring	20.6%	9.5%	<.001

Table 49 comparison 2015/2017 Inexperienced internet user: Victimisation rate

Conscious internet user °2015 – Pessimistic/optimistic experienced internet user °2017

We can see that the victimisation rate for the conscious internet user in 2015 is significantly higher for malware and monitoring than in 2017. This is true for the optimistic experienced internet user as well as the pessimistic experienced internet user. There is, however, no significant difference found for the victimisation of scams and hacking (see table 50).

Cybercrime	**Victimisation percentage 2015**	**Victimisation percentage 2017**		**Significance difference between 2015 & 2017**	
	Conscious internet user	OEI's	PEI's	OEI's	PEI's
Malware	39.6%	18.5%	22.6%	<.001	<.001
Scams	10.7%	9.4%	6.3%	NS	NS
Hacking	13.0%	9.0%	10.4%	NS	NS
Monitoring	30.1%	12.4%	14.5%	<.001	<.001

Table 50 Comparison 2015/2017 conscious internet user/experienced internet users: Victimisation rate

Resolved internet user °2015 – Pessimistic/optimistic defensive internet user °2017

We can see that the victimisation rate for the resolved internet user in 2015 is significantly higher for malware and monitoring than for the optimistic and pessimistic defensive internet users in 2017. There is, however, just like with the OEI's and PEI's no significant difference found for the victimisation of scams and hacking (see table 51).

Cybercrime	**Victimisation percentage 2015**	**Victimisation percentage 2017**		**Significance difference between 2015 & 2017**	
	Resolved internet user	ODI's	PDI's	ODI's	PDI's
Malware	45.4%	10.3%	17.6%	<.001	<.001

Scams	8.7%	4.0%	10.4%	NS	NS
Hacking	14.0%	9.9%	12.9%	NS	NS
Monitoring	26.6%	10.0%	17.1%	<.001	<.05

Table 51 Comparison 2015/2017 resolved internet user/defensive internet users: Victimisation rate

4.4.4 Cybercrime cost

The only cost that is measured in 2015 is the direct monetary cost. Only the victims of a certain cybercrime received the questions about their direct monetary costs after they stated they were victimized. Generally, we can conclude that in 2015 more direct costs were experienced than in 2017 (cfr. Supra). This is also true for every comparable cluster-groups.

Inexperienced internet user °2015 – Inexperienced unknowing internet user °2017

If we compare the inexperienced profiles from 2015 and 2017, we can see for the inexperienced unknowing victims in 2017 more than 80% paid no direct costs for malware, hacking or monitoring whatsoever. For scams, this is not the case with more than 50% of the victims paying “between €20 and €200” or more.

In 2015, however, a direct cost “between €0 and €20” was experienced by more than 75% of the victimized inexperienced internet users for malware, scams, hacking and monitoring. More than 50% of the victims of scams and malware paid “between €20 and €200” or more.

Conscious internet user °2015 – Pessimistic/optimistic experienced internet user °2017

The conscious internet users who were victimized in 2015 also paid more than the 2017 optimistic and pessimistic experienced internet user.

In 2017 more than 60% of the victimized optimistic experienced user paid no money as a direct cost for any cybercrime. 80% of the victimized pessimistic experienced internet user paid no money as a direct cost for malware, hacking or monitoring, for scams, more than 50% of the PEI’s paid “between €20 and €200” or more.

In 2015, the victimized conscious internet users, however, paid much more with more than 50% paying “between €200 and €2000” or more as a direct cost caused by scams. For the other crimes, 75% of them paid between “€0 and €20” or more.

Resolved internet user °2015 – Pessimistic/optimistic defensive internet user °2017

The same story is true when comparing the victimized resolved internet user of 2015 and the victimized pessimistic and optimistic defensive internet user of 2017.

In 2017, more than 80% of the victimized optimistic defensive internet user paid no money as a direct cost caused by any crime. More than 80% of the pessimistic defensive internet user didn’t pay any money as a direct cost for any cybercrimes but scams, for scams more than 25% of them paid “between €20 and €200” or more.

In 2015, more than 75% of the victimized resolved internet user paid “between €0 and €20” or more as a result of every cybercrime. At least 25% of them paid “between €200 and €2000” as a result of scams or hacking. A surprisingly high “more than €2000” was paid by more than 25% of the victimized resolved internet users who were victimized by scams as a direct cost.

We can thus conclude that all clusters from 2015 suffered more direct costs than the comparable clusters from 2017.

4.4.5 Conclusion comparison typology between 2015 and 2017

Comparing the typology of both waves we can highlight some remarkable results.

The IUI’s in 2017 still implement the least security measures

First, the inexperienced internet user (2015) - comparable to the inexperienced unknowing internet user (2017) – now implements the least security measures of all the clusters, while having the same internet diet as in 2015. The victimisation rates for all cybercrimes but hacking and the direct costs for all cybercrimes is lower in 2017 than in 2015 for the inexperienced internet users.

Second, the conscious internet user (2015) - comparable to the pessimistic and optimistic experienced internet user (2017)- are still implementing quite a lot of security measures. They are implementing less maladaptive security measures in 2017 than in 2015. This implicates that they have fewer opportunity costs. As for victimisation, they were victimized significantly less by malware and monitoring in 2017 than in 2015. This is however not significant for scams and hacking. Also, the direct costs they experienced is lower than in 2015

Finally, the resolved internet user of 2015 - comparable to the pessimistic and optimistic defensive internet users (2017)- are implementing more security measures in 2017 than in 2015. The pessimistic defensive internet user (2017), however, implements by far the most maladaptive security measures, compared to the average amount the resolved internet user (2015) implemented maladaptive security measures. This means that the PDI’s are having a lot of opportunity costs in 2017. The optimistic defensive internet user is not implementing maladaptive security measures that much. As for victimisation the 2015 resolved internet user was significantly more victimized on malware and monitoring than the 2017 defensive internet users, this is not so for scams and hacking. Also, the direct costs connected to this victimisation was much higher for the resolved internet user (2015) than for the defensive internet users (2017). The optimistic defensive internet user is an internet user that is optimistic about the internet security and also implements an ample amount of security measures and knows how to do this to keep it this way. The pessimistic defensive internet user, however, is implementing all security measures it can, effective or not, maladaptive or adaptive, it doesn’t matter.

The PDI’s are implementing all security measures they can, effective or not, maladaptive or adaptive

The bad or to little implementation of security measures combined with the big opportunity costs (cfr. Supra) makes the PDI’s together with the IUI’s the clusters of special interest for risk communication.

4.5 PMT-model, predictors of security behaviour (RQ4)

To get a better insight into the process to the intention to implement security measures we used the PMT-model (as outlined in section 2.3). In what follows we discuss the PMT for cybercrime in general, for malware and for scams. We also zoom in on the PMT-model for different typologies of special interest, namely the PDI' and IUI's. Furthermore, we discuss the model-fit, the explanatory value of the model and the predictors of the attitude and intention towards security behaviour.

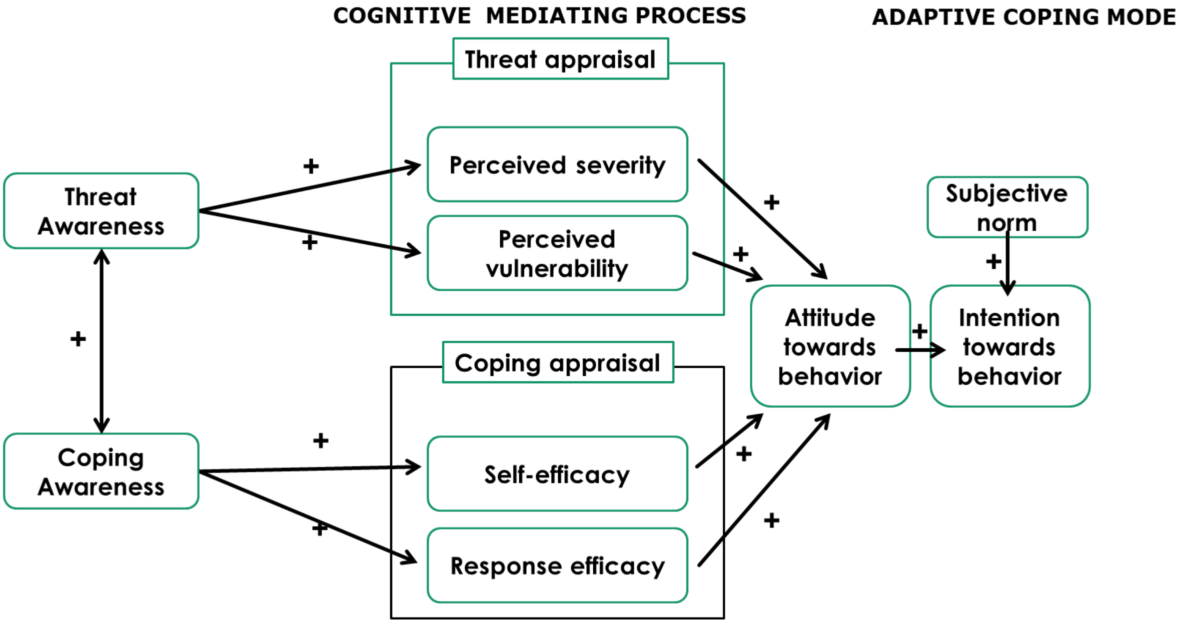


Figure 2: PMT-model

4.5.1 Measuring model

The measuring model has a good fit for the general population (CFI=.922, TLI=.908, RMSEA=.055). See appendix B for the CFA of all measures. They all have strong factor loadings higher than .50. This good fit is also true for the measuring model of malware (CFI=.939 TLI=.923 RMSEA=.054) and scams (CFI=.949 TLI=.940 RMSEA=.053). The CFA is performed for the general population in every occasion. Also here the factor loadings are well above .50. See appendix C and D.

4.5.2 Structural equation model: General population

Bivariate correlations

	1	2	3	4	5	6	7	8
(1) Threat awareness								
(2) Coping awareness	.574**							
(3) Perceived severity	.103**	.119**						
(4) Perceived vulnerability	-.134**	-.183**	.262**					
(5) Self-efficacy	.335**	.470**	-.009	-.252**				
(6) Response efficacy	.183**	.230**	.091**	-.117**	.458**			
(7) Attitude towards behaviour	.229**	.245**	.39**	.058*	.247**	.457**		
(8) Subjective norm	-.094**	-.118**	.106**	.252**	-.075**	.132**	.165**	
(9) Intention towards behaviour	.043	.052	.188**	.240**	-.035	.187**	.329**	.416**

*Table 52: Correlations between study variables (*p<.05 **p<.01)*

In table 52 the correlations between the study variables are displayed. We found significant correlations between all variables. Strong correlations were found between coping awareness and threat awareness (.574**) as was between response efficacy and self-efficacy (.458**). Coping awareness correlates strongly with self-efficacy (.470**). Threat awareness and coping awareness on their turn had no significant correlation with the intention towards taking security measures. Self-efficacy also had no correlation with perceived severity or intention towards taking security measures. All other variables correlated to a greater or lesser extent.

Model Fit

In general, the PMT-models for cybercrime shows an almost good fit looking at a threshold of .90 for the CFI and TLI (CFI=.892, TLI= .880, RMSEA=.063). The model for malware and scams are within parameters for a good fit looking at the goodness-of-fit indices (model malware: CFI=.917, TLI=.901, RMSEA=.061; model scams: CFI=.919, TLI=.911, RMSEA=.065)

Estimates

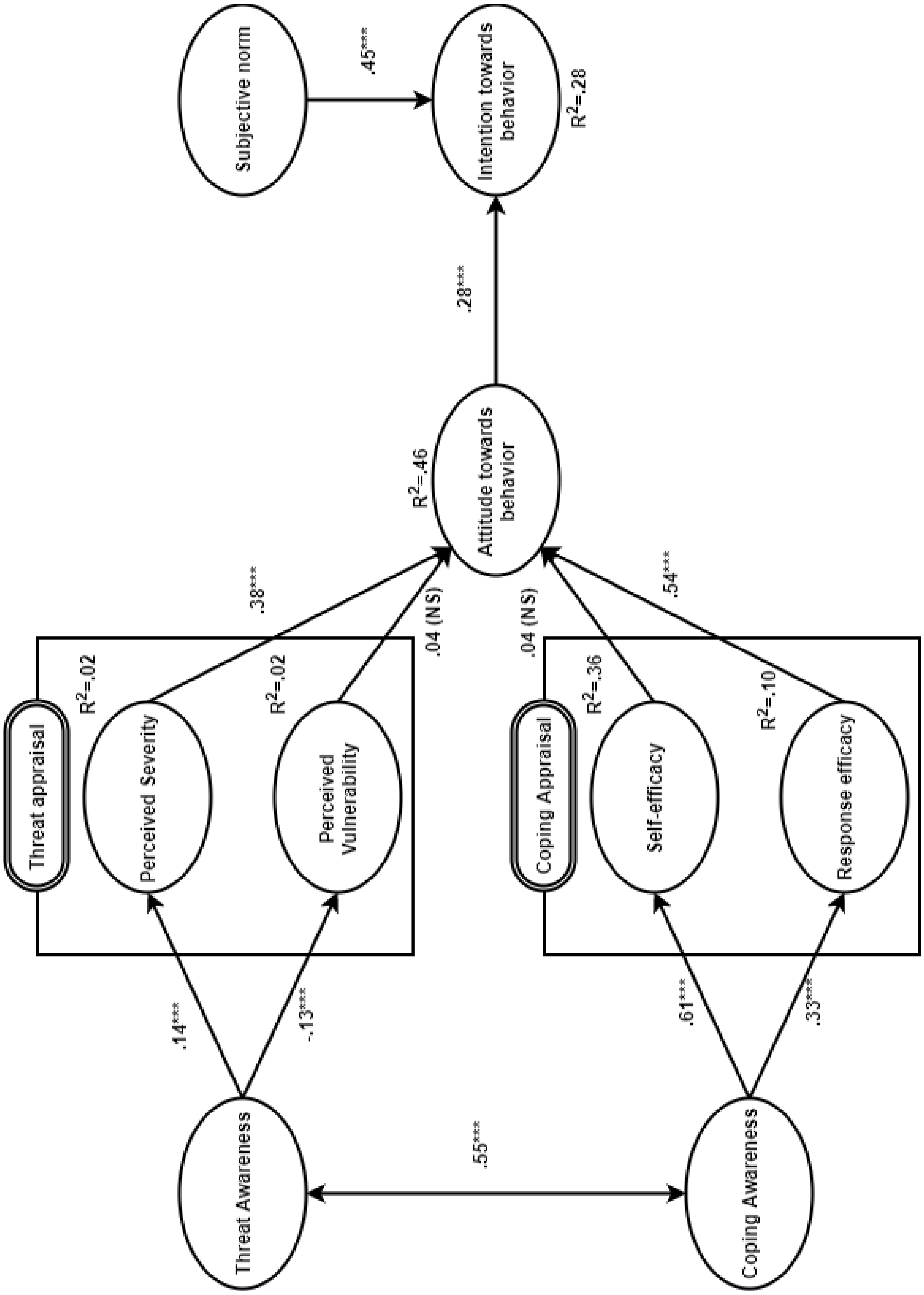


*Figure 1 PMT-model cybercrime in general total population, ***p<.001*

From	To	β (all cybercrimes)	B (Malware)	B(scams)
Threat awareness	**Perceived severity**	.14***	.18***	.03
Threat awareness	**Perceived vulnerability**	-.13***	-.04	-.28***
Coping awareness	**Self-efficacy**	.61***	.61***	.51***
Coping awareness	**Response efficacy**	.33***	.40***	.26***
Self-efficacy	**Attitude towards behaviour**	.04	.01	-.03
Response efficacy	**Attitude towards behaviour**	.54***	.51***	.57***
Perceived vulnerability	**Attitude towards behaviour**	.04	.09***	.02
Perceived Severity	**Attitude towards behaviour**	.38***	.25***	.30***
Attitude towards behaviour	**Intention towards behaviour**	.28***	.29***	.30***
Subjective norm	**Intention towards behaviour**	.45***	.47***	.50***
Explained Variance				
R^2 **(Attitude)**		.46	.34	.41
R^2 **(Intention)**		.28	.31	.34
R^2 **(Perceived Severity)**		.02	.03	.00
R^2 **(Perceived vulnerability)**		.02	.00	.09
R^2 **(Self-efficacy)**		.36	.37	.26
R^2 **(Response efficacy)**		.10	.16	.06

*Table 53 Total sample: Beta's PMT-model by cybercrime ***p<.001*

If we look at the estimations of the different relations in the model we see that a lot of the variables are significantly linked. Furthermore, 46%, 34% and 41% of attitude towards behaviour and 28%, 31% and 34% of intention towards behaviour for all cybercrimes, malware and scams respectively can be explained by our model (see table 53).

Response efficacy and Perceived severity are the strongest predictors of attitude towards behaviour

The strongest predictor that explains the variance in attitude towards behaviour is response efficacy (cybercrime in β_{general}: .54***, β_{malware}=.51***, β_{scams}=.57***), or the feeling that the security measures that are implemented are effective in protecting against cybercrime. However, just a small percentage of it (10% for cybercrime in general, 16% for malware and 6% for scams) is explained by coping awareness.

Perceived severity, or the feeling that a cybercrime is severe, is another good (although less good than response-efficacy) predictor of attitude towards behaviour (cybercrime in β_{general}: .38***, β_{malware}=.25***, β_{scams}=.30***). Perceived severity is, however, also very little explained by threat awareness. This means that making people aware of certain security measures or cybercrime threats is not enough for them to be convinced that these measures are effective or that these cybercrimes are severe. These two are nevertheless the most important predictors of attitude.

Perceived vulnerability, or the feeling of being vulnerable for cybercrimes is only a very weak predictor (β_{malware}=.09***) for attitude towards security behaviour against malware, for scams and cybercrime in general this is not the case. Self-efficacy, or the feeling that they can implement a certain security measure in an effective way is no significant predictor of attitude whatsoever. Self-efficacy, however, is explained a lot for cybercrime in general (36%), malware (37%) and scams (26%) by coping awareness.

Threat awareness is a predictor of perceived severity for cybercrime in general (β_{general}=.14***) and malware (β_{malware}=.18***), this is however not the case for scams. The awareness of scams is thus less important to predict perceived severity. Surprisingly, threat awareness is a significant **negative** predictor of perceived vulnerability for cybercrime in general (β_{general}=-.13**) and scams (β_{general}=-.28**), this is the opposite of what we expected. The more one is aware of cybercrimes and scams, the less vulnerable someone feels.

> *The social pressure towards security behaviour is a stronger predictor than attitude towards behaviour for intention towards behaviour*

The intention toward behaviour is explained for 28% by the attitude towards behaviour and the subjective norm. The most important predictor of the intention to implement security measures is for all three models not the attitude towards behaviour (β_{general}: .28***, β_{malware}=.29***, β_{scams}=.30***) but the subjective norm (β_{general}: .45***, β_{malware}=.47***, β_{scams}=.50***). In other words, the perceived social pressure from others towards security behaviour is more important than attitude as a predictor of intention toward security behaviour.

4.5.3 Structural equation model: Risk typologies

Earlier we stated that the pessimistic experienced internet users and the inexperienced unknowing internet users are the typologies which could benefit the most from risk-communication. Therefore we constructed the three models also for these two clusters to get a better insight.

Pessimistic defensive internet user

In general, the PMT-models for cybercrime applied to pessimistic defensive internet users shows an almost good fit looking at the goodness-of-fit indices (CFI=.906, TLI=.897, RMSEA=.056). The model for malware and scams are also within parameters for a good fit (model malware, CFI=.915, TLI=.899, RMSEA=.064; model scams: CFI=.924, TLI=.915, RMSEA=.063)

From	To	B (all cybercrimes)	B (Malware)	B(scams)
Threat awareness	Perceived severity	.06	.12	-.10
Threat awareness	Perceived vulnerability	-.09	-.05	-.21
Coping awareness	Self-efficacy	.64***	.68***	.52***
Coping awareness	Response efficacy	.44***	.56***	.27***
Self-efficacy	Attitude towards behaviour	-.02	.10	.10
Response efficacy	Attitude towards behaviour	.62***	.35***	.55***
Perceived vulnerability	Attitude towards behaviour	.02	.11	.17
Perceived Severity	Attitude towards behaviour	.26***	.24***	.21***
Attitude towards behaviour	Intention towards behaviour	.30***	.30***	.29***
Subjective norm	Intention towards behaviour	.45***	.56***	.53***
Explained Variance				
R^2 (Attitude)		.45	.24	.39
R^2 (Intention)		.29	.40	.37
R^2 (Perceived Severity)		.00	.01	.01
R^2 (Perceived vulnerability)		.01	.01	.05
R^2 (Self-efficacy)		.38	.45	.26
R^2 (Response efficacy)		.20	.34	.07

*Table 54 PDI: Beta's PMT-model by cybercrime ***p<.001*

PDI's explanatory value of RE is high for cybercrime in general and scams but not for malware

Also for the pessimistic defensive internet users perceived severity and response efficacy are the strongest predictors of attitude towards behaviour (see table 54). Surprisingly though the predictive value of response efficacy takes a nose-dive for malware but not for scams or cybercrime in general (β_{general}: .62***, β_{malware}=.35***, β_{scams}=.55***). A tentative explanation could be that the PDI's are more sceptical towards the efficacy of security measures against malware as they implement the most security measures effective or not (cfr. Supra).

Threat awareness has for the PDI's no predictive value whatsoever, not for perceived severity or perceived vulnerability. However, response efficacy for the PDI's is surprisingly more explained by coping awareness especially for cybercrime in general and malware ($R^2_{all\ cybercrimes}$=.20, $R^2_{malware}$=.34, R^2_{scams}=.07). Coping awareness is thus a good predictor for response efficacy (β_{general}:

.44***, β_{malware}=.56***, β_{scams}=.27***). These insights mean that for PDI's being made aware of the possible security measures (and how to use them) will help their attitude to implement these security measures. This however only holds true to a lesser extent for malware.

Attitude towards behaviour ($R^2_{all\ cybercrimes}$=.45, $R^2_{malware}$=.24, R^2_{scams}=.39) and intention towards behaviour ($R^2_{all\ cybercrimes}$=.29, $R^2_{malware}$=.40, R^2_{scams}=.37) are explained in line with the population in general.

Just like the general population, the subjective norm (β_{general}: .45***, β_{malware}=.56***, β_{scams}=.53***) is a better predictor than attitude towards behaviour (β_{general}: .30***, β_{malware}=.30***, β_{scams}=.29***) for intention towards behaviour.

Inexperienced unknowing internet users

In general, the PMT-models for cybercrime applied to the inexperienced unknowing internet users shows an equal almost good fit looking at the goodness-of-fit indices (CFI=.878, TLI=.866, RMSEA=.066). The model for malware and scams are also an almost good fit according to the goodness-of-fit indices (model malware: CFI=.905, TLI=.887, RMSEA=.065; model scams: CFI=.901, TLI=.891 RMSEA=.072).

From	To	B (all cybercrimes)	B (Malware)	B(scams)
Threat awareness	**Perceived severity**	.14	.23*	.05
Threat awareness	**Perceived vulnerability**	.03	.11	-.14
Coping awareness	**Self-efficacy**	.45***	.47***	.38***
Coping awareness	**Response efficacy**	.24***	.35***	.22**
Self-efficacy	**Attitude towards behaviour**	-.05	-.07	-.11
Response efficacy	**Attitude towards behaviour**	.59***	.60***	.54***
Perceived vulnerability	**Attitude towards behaviour**	.10	.16**	.09
Perceived Severity	**Attitude towards behaviour**	.38***	.17**	.32***
Attitude towards behaviour	**Intention towards behaviour**	.31***	.30***	.26***
Subjective norm	**Intention towards behaviour**	.53***	.50***	.55***
Explained Variance				
R^2 (Attitude)		.51	.42	.40
R^2 (Intention)		.37	.34	.37
R^2 (Perceived Severity)		.03	.06	.01
R^2 (Perceived vulnerability)		.00	.01	.03
R^2 (Self-efficacy)		.20	.25	.13
R^2 (Response efficacy)		.05	.11	.04

*Table 55 IUI: Beta's PMT-model by cybercrime ***p<.001 **p<.01 *p<.05*

In line with the general population and the PDI's, response efficacy (β_{general}: .59***, β_{malware}=.60***, β_{scams}=.54***) and perceived severity (β_{general}: .38***, β_{malware}=.17***, β_{scams}=.32***) are good predictors of attitude to take security measures against cybercrime for the inexperienced unknowing internet users (see table 55).

> *Perceived vulnerability is a weak predictor of attitude towards security behaviour against malware for the IUI's*

The explanatory value of response efficacy here stays very high for cybercrime in general, malware and scams. Perceived severity ($R^2_{all\ cybercrimes}$=.03, $R^2_{malware}$=.06, R^2_{scams}=.01) and response efficacy ($R^2_{all\ cybercrimes}$=.05, $R^2_{malware}$=.11, R^2_{scams}=.04) are for the IUI's less explained by coping awareness or threat awareness than for the general population or the pessimistic defensive internet users. This means that just making the IUI aware of threats and security measures won't be enough to change the perceived severity and response efficacy of the IUI's. We should thus search for more predictors as response efficacy and perceived severity are still very strong predictors for attitude towards behaviour (cfr. Supra).

Perceived vulnerability is for the IUI's a weak predictor (β_{malware}=.16***) of the attitude towards security behaviour against malware, this is not the case for cybercrime in general or scams. This is, however, only for the IUI's significant.

The subjective norm (β_{general}: .53***, β_{malware}=.50***, β_{scams}=.55***) also here stays a better predictor than attitude towards behaviour (β_{general}: .31***, β_{malware}=.30***, β_{scams}=.26***) for intention towards behaviour ($R^2_{all\ cybercrimes}$=.37, $R^2_{malware}$=.34, R^2_{scams}=.37).

Comparison between2017 and 2015 SEM analysis of PMT-model

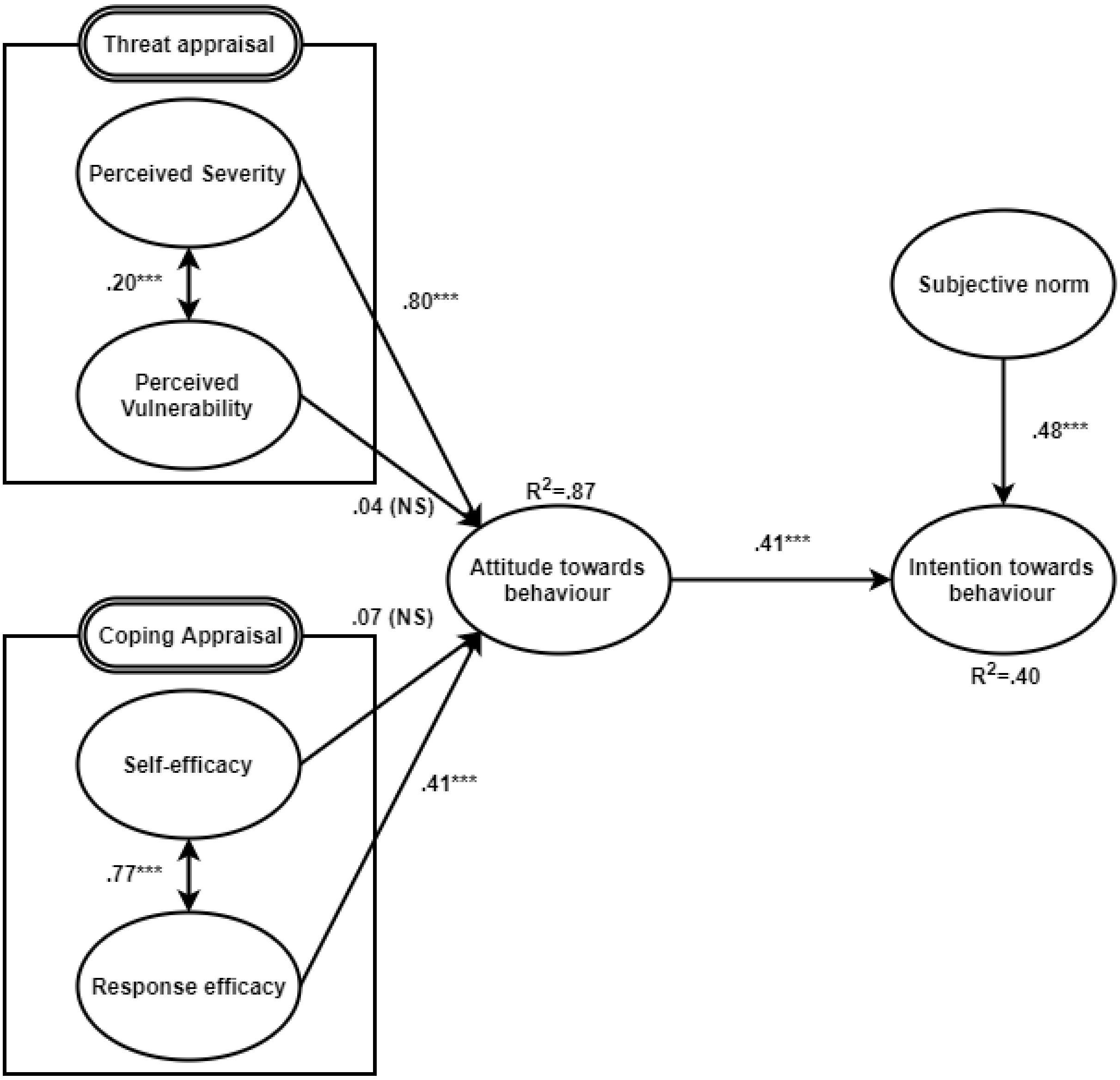


Figure 2 PMT-model 2015 (n=1033)

> *Attitude towards behaviour is in 2017 a less strong predictor than in 2015 for intention towards behaviour*

The model of 2015 also reached an almost good fit (CFI=.869, TLI=.850, RMSEA=.078), If we look at the SEM analysis of the PMT model proposed in 2015 we see that the same was true. Response efficacy and perceived severity were the important predictors of attitude towards security behaviour. It is however noticeable that attitude towards behaviour now is a less good predictor than in 2015. In 2017 $\beta_{attitude \rightarrow intention}$=.28**** and in 2015 $\beta_{attitude \rightarrow intention}$=.41****. Attitude towards behaviour was much more explained in 2015 by perceived severity and response efficacy. This means that there could be more predictors in 2017 that predict attitude towards behaviour. Subjective norm stayed the same strong predictor of intention towards behaviour ($\beta_{subjective\ norm \rightarrow intention}$=.48***).

4.5.4 Conclusion PMT model

We can conclude that perceived severity and response efficacy are good predictors of attitude towards security behaviour. The other constructs (Perceived vulnerability and self-efficacy) are less good predictors. This means that in general people have a higher attitude towards implementing security measures if they perceive the threat as severe (perceived severity) and if they think their security measures are effective (response efficacy). Feeling that they are able to implement these security measures (self-efficacy) or that they are vulnerable to be victimized by cybercrime (perceived vulnerability) has less effect on the attitude towards implementing security measures. This attitude is in its turn -together with the subjective norm- a good predictor of the intention towards security behaviour. In general, a good part of intention and attitude is explained by the proposed PMT-model. It is however interesting to see that perceived severity and response efficacy is explained very little in current PMT-model by threat and coping awareness, this is especially true for the inexperienced unknowing internet users and the population in general. This means that coping and threat awareness are not the only predictor of perceived severity and response efficacy and thus that there are other constructs that additionally could play a predicting role. Searching and finding these predictors could demystify the process towards the intention to implement security measures even further and could help risk communication towards the IUI’s.

This makes room for further research to track down what influences the perceived severity and response efficacy of someone. Furthermore, it seems interesting to search for other constructs predicting the attitude towards security behaviour.

5 Discussion

5.1 Main results

In general, the internet is used most for information linked activities like checking emails, retrieving information, searching news sites and using social network sites. The Belgian population also uses the internet for electronic banking, but to a lesser extent.

Looking at the perceived safety of the online activities, downloading, using social network sites and online games are considered the least safe. Electronic banking, retrieving information, visiting news sites and email are considered the safest of online activities.

Most people seem to be aware of the dangers of the internet and are implementing quite a lot of security measures to protect themselves against cybercrime. This, however, doesn't hold up for the inexperienced internet users, who are the least aware of cybercrime threats and security measures, and are implementing the least security measures.

In 2017, people are implementing more technological adaptive security measures and less maladaptive security measures than in 2015. However, over 5% of the population do not implement any security measure against any cybercrime in 2017. Even stronger, 25% of the population do not take any action against monitoring. People who do not know if they were victimized, implement significantly fewer security measures. Hereby, they are also more likely to be a carrier of malware or other cybercrimes without knowing or even planning to do something about it. Therefore, they should be considered to be especially vulnerable. A risk awareness campaign could help educate these people (see 5.2 recommendations for risk communication).

Cybercrime in general still makes a lot of victims. Malware and monitoring however made significantly fewer victims in 2017 than in 2015. There is a large group of people who do not know if they were victimized in 2017, the same was true in 2015. Malware makes the most victims in general, but scams cause for the highest monetary costs. Monitoring is considered to be the least expensive. For all the cybercrimes but scams, more than 80% of the victims suffered no direct costs in 2017. The monetary direct costs in 2017 are significantly lower than in 2015.

For defence cost, people pay the most for malware and hacking. These are, however, not the most expensive cybercrimes in terms of direct monetary costs. Direct non-monetary costs are not significantly different for the different cybercrimes.

In 2017, we differentiated between five clusters compared to four clusters in 2015. These clusters are: optimistic defensive internet users (ODI), pessimistic defensive internet users (PDI), inexperienced unknowing internet users (IUI), optimistic experienced internet users (OEI) and pessimistic experienced internet users (PEI).

In the data we can further differentiate on their internet diet: novice internet users, intermediate internet users and advanced internet users. IUI's are generally novice internet users, PDI's and ODI's are generally intermediate internet users, OEI's and PEI's are more advanced internet users. The breakdown into these three bigger groups also holds up when considering their security measures. The novice internet users implement the least security measures, followed by the advanced internet users and the intermediate internet users. The PEI's and OEI's don't differ significantly in their security behaviour. The PDI's and ODI's implement the same amount of adaptive security measures. The PDI's, however, use the most (and significantly more than the rest) maladaptive security measures. This could indicate bigger opportunity losses as these maladaptive security measures include stopping or reducing internet usage and stopping or reducing certain activities online.

The PDI's are significantly more victimized by hacking and monitoring and are the most victimized by scams (although not significantly more than the rest). This means that their security measures are not really effective as they do implement the most security measures. The IUI's are surprisingly victimized less often than expected by hacking and monitoring. They are however also significantly less aware of cyberthreats and security measures, these results lend to support that they are not able to notice when they are victimized or not. PEI's are more victimized by malware then we would expect, this could be explained by the fact that s/he uses the internet more often and in a more advanced way and thus encounters more cybercrimes.

The IUI's implement the least security measures, have relatively the most victims paying and pay the most money as a consequence of scams. Victimisation rate, however, is not linked to the amount someone pays as a direct cost following a victimisation event.

Opportunity costs are believed to be felt by every cluster but the OEI's. Especially the PEI's and the IUI's perceive most opportunity costs.

The combination of the reduction in victimisation rate of malware and monitoring and an increase of technical adaptive security measures makes us believe that people in 2017 are better armed against cyber criminality than in 2015. The victimisation of scams and hacking, however, hasn't changed in a significant way, despite the growing security measures that are used. Overall, the direct monetary costs have declined compared to 2015.

Considering the PMT-model, we see that the perceived severity and response efficacy are the most important predictors of attitude towards security behaviour for the general population for cybercrime in general. The other constructs are less good predictors. This means that people who perceive a certain threat as severe (perceived severity) and or think their security measure is effective (response efficacy) have a higher attitude towards implementing these security measures. How good they themselves are in implementing this security measures (self-efficacy) or how much chance there is to get victimized (perceived vulnerability) is less important as these have no significant predictive value. Except for malware with the IUI's where the perceived vulnerability is a significant predictor of attitude. Only a small percentage of perceived severity and response efficacy, however, is explained by threat- and coping awareness. Attitude towards security behaviour is explained for 46% by response efficacy and perceived severity.

Together with the subjective norm, attitude towards behaviour explains 28% of the intention towards implementing security measures against cybercrime in general. It is, however, important to note that subjective norm is a stronger predictor than the attitude towards behaviour for intention.

5.2 Recommendations for risk communication

The OEI's and PDI's are the two clusters that are of special interest for risk communication if we look at the victimisation rate combined with the security measures. This does not mean the other clusters don't need or could benefit from risk communication.

5.2.1 Recommendations to reach out to inexperienced unknowing internet users

In line with the results of 2015, we believe the IUI's to be an important target group because they are not cognizant of being a victim or not; they are significantly less aware of cybercrime threats and security measures that can be used. On top of that, they experience many opportunity costs.

Considering the PMT-model we can conclude that social norm can be seen as the strongest predictor to change the behaviour of the IUI's to implement security behaviour. Also, attitude towards this security behaviour can be seen as an important though less strong predictor of this security behaviour.

Attitude towards taking security behaviour is being influenced mainly by response efficacy and perceived severity. With other words to facilitate a shift in attitude with the IUI's, you should mainly convince them that the security actions they take are effective in protecting them and that the harm they could experience if they are victimized by cybercrime is severe. The feeling that they are able to implement these security measures themselves (self-efficacy) or that they are vulnerable to get victimized by cybercrime (perceived vulnerability) is less important to change the attitude towards security behaviour. Only with malware, the feeling of being vulnerable to get victimized plays a role in the attitude towards taking security behaviour against malware.

Making the IUI's aware of the cybercrimes and security measures is not enough to facilitate a shift in response efficacy and perceived severity. When reaching out to IUI's, you should explain the substantial risk of the different cybercrimes and educate them on how to take effective security measures. It is also important not to increase their opportunity risks while educating them of the severity of the risks, this would increase the digital divide already existing.

5.2.2 Recommendations to reach out to pessimistic defensive internet users

The PDI's are believed to be another important target group. They implement many security measures but are doing this in an ineffective way. They still report to be victimized and experience a lot of opportunity costs trying to protect themselves.

Considering the PMT-model we can conclude just as with the IUI's that also here social norm can be seen as the strongest predictor followed by the attitude towards security behaviour to implement security behaviour.

Attitude towards taking security behaviour is also here being influenced mainly by response efficacy and perceived severity. However, the predictive value of response efficacy takes a nose dive with malware. Taking into account that the PDI's implement the most security measures, effective or not, this means that to facilitate a shift in attitude with the PDI's, you should mainly convince them that, and explain to them which, security actions are effective in protecting them against cybercrime. Furthermore, it is also important to convince them of the severeness of being victimized to facilitate a shift in attitude towards security behaviour.

The feeling that they are able to implement these security measures themselves (self-efficacy) or that they are vulnerable to get victimized by cybercrime (perceived vulnerability) are also with the PDI's less important to change the attitude towards security behaviour.

Making the PDI's aware of the security measures they can take is having a high impact on the response efficacy for all cybercrimes but scams. This, however, is not enough to ensure the PDI's implement these security measures in an effective way. Therefore, it is important to explain to the PDI's what security measures are effective to take and what security measures are ineffective and should be avoided to minimize opportunity costs. Making them aware of the cybercrimes that exist have no influence whatsoever and is thus not necessary.

5.2.3 Recommendations for the other typologies

If we look at the ODI's we see they mainly experience opportunity costs. We should inform them more about what is and what isn't a risky behaviour online. Especially with more than half of the ODI's perceiving every online activity as neutral or safer (including downloading).

ODI's, PDI's and IUI's are novice to intermediate internet users. With the increasing media attention for cybercrime, it seems important to also make sure that less internet savvy people are not getting left behind because of opportunity costs and victimisation by cybercrime. Also, PEI's are experiencing these opportunity costs.

PEI's and OEI's should not be forgotten when informing about the safety in online behaviour especially because they engage more often and in more advanced activities online and are thus more often being exposed to cybercrime.

5.3 Scope, limitations of the research and future research

This study adds to the research about internet users' intention to take security measures against cybercrime. It builds further on the research executed in 2015 with the same basic framework, namely the PMT-model. This research adds by extending the PMT-model with threat awareness and coping awareness as proposed in the previous wave and implemented in other research (Hanus & Wu, 2016; Verdegem et al., 2015).

The results of this research and the research of 2015 confirm that the PMT framework is a good framework to analyse the process of taking security measures against cybercrime. This study finds a significant relation between perceived severity and attitude towards security behaviour and response efficacy and attitude towards security behaviour. This relationship was also uncovered with the data of the 2015 survey. If we make a longitudinal comparison we can see that perceived severity and response efficacy, however, explained more of the attitude towards security behaviour in 2015 than in 2017. The coping awareness that is added in 2017 has a significant relation with response efficacy. The threat awareness, however, is not a significant predictor of perceived severity, except for the inexperienced unknowing internet users where it does significantly predict the perceived severity of malware.

By dividing the costs linked to cybercrime in direct monetary cost, direct non-monetary costs, opportunity costs and defence costs we were able to get a more fine-grained image of the costs connected to cybercrime. because the high amount of people paying nothing when victimized and the relative low victimisation rates, however, it was impossible to get a clear number on the average amount of direct monetary or even defence costs. It is clear that opportunity costs are perceived quite often by everyone but the optimistic experienced internet users. There was no difference found between the clusters in terms of the non-monetary direct costs operationalized by the harm-assessment framework (Greenfield & Paoli, 2013). This could indicate that the harm-assessment framework is not fine-grained enough in the context of citizen-research.

The limitations of our study made it impossible to know how security measures were implemented. This way we couldn't know if security measures were effectively implemented or not. The pessimistic defensive internet users for example show by far the most implemented security measures but are still victimized the most by many cybercrimes. Future research could assess the implemented security measures in a more qualitative manner.

With direct costs only being experienced by victims, more specified research should be executed towards victims to get a better insight into these direct costs. The results for direct costs of this research is only of an exploratory nature.

Furthermore, it was impossible in our study to find out if the amount of security measures and the perceived opportunity costs were a result of previous victimisation or if they were already present before the victimisation. This would implicate totally different conclusions. Future research might increase our insight into the decision-making process to implement certain security measures and this way demystify this limitation.

To broaden and strengthen the PMT-model, more constructs should be added and tested. Especially constructs that influence perceived severity and response efficacy are of exceptional interest. Furthermore, it would be interesting to get a better insight into how the subjective norm is formed as this was a strong predictor of intention towards security behaviour in the research of 2015 and in current research.

A broader scope of this research area should also implement IoT devices as these are becoming more and more mainstream and therefore are bringing more risks.

6 Bibliography

Agrafiotis, I., Bada, M., Cornish, P., Creese, S., Goldsmith, M., Ignatuschtschenko, E., … Upton, D. (2016). Cyber Harm : Concepts, Taxonomy and Measurement. *Said Business School Research Papers*, *23*(8), 1–45.

Anderson, R., Barton, C., Bhöme, R., Clayton, R., Van Eeten, M., Levi, M., … Savage, S. (2013). Measuring the Cost of Cybercrime: a workshop. *The Economics of Information Security and Privacy*, 265–300.

Armin, J., Thompson, B., Ariu, D., Giacinto, G., Roli, F., & Kijewski, P. (2015). 2020 cybercrime economic costs: No measure no solution. *10th International Conference on Availability, Reliability and Security, ARES 2015*, 701–710. https://doi.org/10.1109/ARES.2015.56

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance*, *28*(April), 24–31. https://doi.org/10.1016/S2212-5671(15)01077-1

Brownson, R., Chang, J., Eyler, A., Ainsworth, B., Kirtland, K., & Sallis, J. (2004). Measuring the environment for friendliness toward physical activity: A comparison of the reliability of 3 quesionnaires. *American Journal of Public Health*, *94*(3), 473–483.

Centraal bureau voor statistiek. (2017). *Veiligheidsmonitor 2016*.

Choi, K.-S. (2008). Computer Crime Victimization and Integrated Theory: An Empirical Assessment. *International Journal of Cyber Criminology*, *2*(1), 308–333.

Chou, H. L., & Sun, J. C. Y. (2017). The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers and Education*, *112*, 83–96. https://doi.org/10.1016/j.compedu.2017.05.003

Couts, A. (2014). NSA pretended to be Facebook in its effort to infect “millions” of computers. Retrieved November 8, 2017, from https://www.digitaltrends.com/web/nsa-pretended-facebook-spread-malware/

Crossler, R., & Bélanger, F. (2014). An Extended Perspective on Individual Security Behaviors. *ACM SIGMIS Database*, *45*(4), 51–71. https://doi.org/10.1145/2691517.2691521

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers and Security*, *48*(February 2015), 281–297. https://doi.org/10.1016/j.cose.2014.11.002

De Jonge, J., Van Trijp, H., Renes, R., & Frewer, L. (2007). Understanding consumer confidence in the safety of food: Its two-dimensional structure and determinants. *Risk Analysis*, *27*(3), 729–740. https://doi.org/10.1111/j.1539-6924.2007.00917.x

Dinev, T., Hart, P., & Mullen, M. R. (2008). Internet privacy concerns and beliefs about government surveillance - An empirical investigation. *Journal of Strategic Information Systems*, *17*(3), 214–233. https://doi.org/10.1016/j.jsis.2007.09.002

Dodel, M., & Mesch, G. (2017). Cyber-victimization preventive behavior: A health belief model approach. *Computers in Human Behavior*, *68*(December 2016), 359–367. https://doi.org/10.1016/j.chb.2016.11.044

Europol. (2017). *Internet Organised Crime Threat Assessment 2017*. https://doi.org/10.2813/55735

Eurostat. (2016). *Eurostat model for the EU survey on ICT usage in households and by individuals 2015, version 3.1*.

FOD Economie. (2017). Bevolking en mobiliteit. Retrieved November 8, 2017, from http://statbel.fgov.be/nl/statistieken/bestat/#4

Froomkin, A. M. (2015). Regulating mass surveillance as privacy pollution: Learning from environmental impact statements. *University of Illinois Law Review*, *2015*(5), 1713–1790. https://doi.org/10.2139/ssrn.2400736

Greenfield, V. A., & Paoli, L. (2013). A framework to assess the harms of crimes. *British Journal of Criminology*, *53*(5), 864–885. https://doi.org/10.1093/bjc/azt018

Hanus, B., & Wu, Y. Andy. (2016). Impact of Users' Security Awareness on Desktop Security Behavior: A Protection Motivation Theory Perspective. *Information Systems Management*, *33*(1), 2–16. https://doi.org/10.1080/10580530.2015.1117842

Henson, B., Reyns, B. W., & Fisher, B. S. (2016). Cybercrime victimization. In *The Wiley handbook on the psychology of violence.* (pp. 555–570).

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems*, *18*(2), 106–125. https://doi.org/10.1057/ejis.2009.6

Holt, T. J., & Bossler, A. M. (2008). Examining the Applicability of Lifestyle-Routine Activities Theory for Cybercrime Victimization. *Deviant Behavior*, *30*(1), 1–25. https://doi.org/10.1080/01639620701876577

Holt, T. J., & Bossler, A. M. (2014). An Assessment of the Current State of Cybercrime Scholarship. *Deviant Behavior*, *35*(1), 20–40. https://doi.org/10.1080/01639625.2013.822209

Internet live stats. (2017). Internet users. Retrieved November 8, 2017, from http://www.internetlivestats.com/internet-users-by-country/

Interpol. (2017). Cybercrime. Retrieved November 8, 2017, from https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Jansen, J., & van Schaik, P. (2017). Comparing three models to explain precautionary online behavioural intentions. *Information and Computer Security*, *25*(2), 165–180. https://doi.org/10.1108/ICS-03-2017-0018

Jansen, J., Veenstra, S., Zuurveen, R., & Stol, W. (2016). Guarding against online threats: Why entrepreneurs take protective measures. *Behaviour & Information Technology*, *35*(5), 368–379. https://doi.org/10.1080/0144929X.2016.1160287

Lagazio, M., Sherif, N., & Cushman, M. (2014). A multi-level approach to understanding the impact of cybercrime on the financial sector. *Computers & Security*, *45*, 58–74. https://doi.org/10.1016/j.cose.2014.05.006

Leukfeldt, E. R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*(3), 263–280. https://doi.org/10.1080/01639625.2015.1012409

Li, X. (2016). Taxonomy of Cybercrime. *Journal of Legal Studies*, *1*(1), 1–27.

Liptak, A. (2017). The WannaCry ransomware attack has spread to 150 countries. Retrieved November 8, 2017, from https://www.theverge.com/2017/5/14/15637888/authorities-wannacry-ransomware-attack-spread-150-countries

Lynley, M. (2017). Equifax was reportedly hacked almost five months before its first disclosed date. Retrieved November 8, 2017, from https://techcrunch.com/2017/09/18/equifax-was-reportedly-hacked-almost-five-months-before-its-first-disclosed-date/

Lyon, D. (2014). Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, *1*(2), 1–13. https://doi.org/10.1177/2053951714541861

Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2010). potential factors of online victimization of youth: an examination of adolescent online behaviors utilizing routine activity theory. *Deviant Behavior*, *31*(5), 381–410. https://doi.org/10.1080/01639620903004903

Martellini, M., Abaimov, S., Gaycken, S., & Wilson, C. (2017). *Information Security of Highly Critical Wireless Networks*. *SPRINGER BRIEFS IN COMPUTER SCIENCE*.

Meso, P., Ding, Y., & Xu, S. (2013). Applying Protection Motivation Theory to Information Security Training for College Stude. *Journal of Information Privacy & Security*, *9*(5), 47–67. https://doi.org/10.1080/15536548.2013.10845672

Milne, S., Sheeran, P., & Orbell, S. (2000). Prediction and Intervention in Health-Related Behavior: A Meta-Analytic Review of Protection Motivation Theory. *Journal of Applied Social Psychology*, *30*(1), 106–143.

Ngo, F., & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773–793.

NSA posed as Facebook in effort to infect “millions” of computers with malware, Snowden documents reveal. (2014, March 13). Retrieved September 2, 2015, from http://www.dailymail.co.uk/news/article-2579836/NSA-posed-Facebook-effort-infect-millions-computers-malware-Owning-Net-program-stolen-documents-reveal.html

OECD (2017), Adult education level (indicator). doi: 10.1787/36bce3fe-en (Accessed on 07 November 2017)

Paoli, L., Visschers, J., Verstraete, C., & van Hellemons, E. (2017). *The Impact of Cybercrime on Business. Whitepaper*.

Rens, B. (2015). A routine activity perspective on online victimisation. *Journal of Financial Crime*, *22*(4), 396–411. https://doi.org/10.1108/JFC-06-2014-0030

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being Pursued Online: Applying cyberlifestyle-Routine Activities Theory to Cyberstalking Victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169. https://doi.org/10.1177/0093854811421448

Reyns, B. W., Randa, R., & Henson, B. (2016). Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety*, *18*(1), 38–59. https://doi.org/10.1057/cpcs.2015.21

Riek, M., Böhme, R., & Moore, T. (2016). Measuring the Influence of Perceived Cybercrime Risk on Online Service Avoidance. *IEEE Transactions on Dependable and Secure Computing*, *13*(2), 261–273. https://doi.org/10.1109/TDSC.2015.2410795

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Shillair, R., Cotten, S. R., Tsai, H. Y. S., Alhabash, S., Larose, R., & Rifon, N. J. (2015). Online safety begins with you and me: Convincing Internet users to protect themselves. *Computers in Human Behavior*, *48*(12), 199–207. https://doi.org/10.1016/j.chb.2015.01.046

Sommestad, T., Karlzén, H., & Hallberg, J. (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy*, *9*(1), 26–46.

Stabek, A., Watters, P., & Layton, R. (2010). The seven scam types: Mapping the terrain of cybercrime. In *Proceedings - 2nd Cybercrime and Trustworthy Computing Workshop, CTC 2010* (pp. 41–51). https://doi.org/10.1109/CTC.2010.14

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a "Digital Criminology"? *International Journal for Crime, Justice and Social Democracy*, *6*(2), 17–33. https://doi.org/10.5204/ijcjsd.v6i2.355

Tsai, H. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Tsakalidis, G., & Vergidis, K. (2017). A Systematic Approach Toward Description and Classification of Cybercrime Incidents. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *PP*(99), 1–20. https://doi.org/10.1109/TSMC.2017.2700495

Vakhitova, Z. I., Reynald, D. M., & Townsley, M. (2016). Toward the Adaptation of Routine Activity and Lifestyle Exposure Theories to Account for Cyber Abuse Victimization. *Journal of Contemporary Criminal Justice*, *32*(2), 169–188. https://doi.org/10.1177/1043986215621379

Van der Hulst, R. C., & Neve, R. J. M. (2008). *High-tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie*.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from Habit and Protection Motivation Theory. *Information and Management*, *49*(3–4), 190–198. https://doi.org/10.1016/j.im.2012.04.002

Vanhaelewyn, B., & De Marez, L. (2016). *Digimeter 2016. Measuring digital media trends in Flanders*. Retrieved from http://www.imec-int.com/en/digimeter-2016/download

Verdegem, P., Teerlinck, E., & Vermote, E. (2015). *Measuring Cost and impact of cybercrime in Belgium (BCC): D.3.1.1. Risk Perception Monitor Report (1st wave, 2015)*. Ghent.

Wickramasekera, N., Wright, J., Elsey, H., Murray, J., & Tubeuf, S. (2015). Cost of crime: A systematic review. *Journal of Criminal Justice*, *43*, 218–228. https://doi.org/10.1016/j.jcrimjus.2015.04.009

World Economic Forum. (2015). *Deep shift: technology tipping points and societal impact*. *World Economic Forum*. Retrieved from http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf

Appendix A: Operationalising, Mean, Standard deviation and Cronbach's alpha

Construct	Question in survey	Answer Options	Mean	SD	Cronbach's α
Gender	What is your gender?	Man/Woman/Other			
Birth year	In what year were you born? (e.g. 1985)	Open			
Residence	Where do you live?	Flanders/Wallonia/Brussels			
Language	What language do you speak?	Dutch/French/English			
Profession	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:			
Diploma	What is your highest diploma?	No diploma Primary Lower secondary Upper secondary (ASO) Upper secondary technical and art (TSO/KSO) Upper secondary vocational (BSO) Higher non-university/Bachelor (Post)graduate/ Master			
Family situation	What best describes your family situation? Minors are children under 18.	Married/living together without minor children Married/living together with			

		minor children Single without minor children Single with minor children Living with parent(s)/relatives Living with others Student in student accommodation/digs			
Internet_device	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) Smart TV Other: None of the above			
Internet_activity	Which of the following activities have you done in the last month using your device(s)? (multiple answers are possible). Question is asked for every indicated device in “Internet_device”	To retrieve information To visit news sites To E-mail To do online banking To online game (e.g. games on Facebook, multiplayer games on a console...) To use social media (e.g. Facebook, Twitter, Instagram, Snapchat...) To chat To conduct phone calls over the internet (e.g. Skype, Facetime, Duo...)			

		To purchase and/or sell goods online (e.g. Music, movies, software, books, clothing...) To download (e.g. music, movies, software, books...) To stream (play files without downloading them e.g. youtube, Spotify, Netflix, Popcorn Time...)			
Internet_usage_place	How often do you use the internet in a typical week? 1. At home during work days 2. At home during weekend 3. At work	Never Less than weekly Less than daily Less than 1 hour per day Between 1 and 3 hours per day Between 3 and 5 hours per day Between 5 and 8 hours per day More than 8 hours per day	1. 5,21 2. 5,36 3. 3,36	1. 1,048 2. 1,109 3. 2,370	
Internet_activity_frequency	Which of the following activities have you done in the last month using your device(s)? (multiple answers are possible) 1. To retrieve information 2. To visit news sites 3. To E-mail 4. To do online banking 5. To online game (e.g. games on Facebook, multiplayer games on a console...) 6. To use social media (e.g. Facebook, Twitter, Instagram, Snapchat...) 7. To chat	Never At least yearly At least monthly At least weekly At least daily More than once every day	1. 4,97 2. 4,94 3. 5,10 4. 3,69 5. 2,60 6. 4,27 7. 2,84 8. 2,16 9. 2,40 10. 2,02 11. 2,81	1. 0,916 2. 1,091 3. 0,942 4. 0,975 5. 1,896 6. 1,906 7. 1,905 8. 1,372 9. 0,900 10. 1,173 11. 1,608	

	8. To conduct phone calls over the internet (e.g. Skype, Facetime, Duo...) 9. To purchase and/or sell goods online (e.g. Music, movies, software, books, clothing...) 10. To download (e.g. music, movies, software, books...) 11. To stream (play files without downloading them e.g. youtube, Spotify, Netflix, Popcorn Time...)				
Internet_safety_general	To what extent do you agree with the following statements? 1. I am optimistic about the safety of the internet. 2. I am concerned about internet safety. (Inverted) 3. I have every confidence that the internet is safe. 4. I am satisfied with the safety of the internet.	5 point likert scale (totally disagree – totally agree)	1. 2,76 2. 2,38 3. 2,46 4. 2,80	1. 0,938 2. 0,921 3. 0,917 4. 0,879	0,850
Internet_safety_activities	How safe do you think these activities are in general? 1. To retrieve Information 2. To visit news sites 3. To e-mail 4. To do online banking 5. To online game (e.g. games on Facebook, multiplayer games on a console...) 6. To use social media (e.g. Facebook, Twitter, Instagram, Snapchat...) 7. To chat	Not safe at all – Not Safe – Neutral – Safe – Very Safe – I don’t know	1. 3,39 2. 3,60 3. 3,44 4. 3,39 5. 2,59 6. 2,58 7. 2,80 8. 3,15 9. 2,94 10. 2,33 11. 2,85	1. 0,961 2. 0,959 3. 0,958 4. 1,185 5. 1,038 6. 0,999 7. 1,017 8. 0,946 9. 0,995 10. 0,969 11. 1.043	0,900

	8. To conduct phone calls over the internet (e.g. Skype, Facetime, Duo...) 9. To purchase and/or sell goods online (e.g. Music, movies, software, books, clothing...) 10. To download (e.g. music, movies, software, books...) 11. To stream (play files without downloading them e.g. youtube, Spotify, Netflix, Popcorn Time...)				
Threat_awareness	How aware are you of the following concepts? 1. Malware 2. Scams 3. Hacking 4. Monitoring	Totally not aware – Not aware - Neutral – Aware – Totally aware	1. 3,02 2. 3,72 3. 3,60 4. 3,11	1. 1,361 2. 1,062 3. 1,075 4. 1,225	0,839
Coping_awareness	How aware are you with these countermeasures? (if you are aware of a software pack that cover more than one countermeasure (e.g. an automatic password generator, anti-virus and backup program in one.) you can thick the box with every countermeasures.) 1. Instal software e.g. anti-virus, anti-spyware, anti-phishing, cryptolocker, backup software 2. Set up software that is included with your operating system (e.g. firewall, defender) 3. Update software en operating systems 4. Secure a wifi network 5. Set up difficult to guess passwords for accounts and home network	Totally not aware – Not aware - Neutral – Aware – Totally aware	1. 3,79 2. 3,42 3. 3,64 4. 3,31 5. 3,83 6. 3,34 7. 4,04 8. 3,05 9. 3,14	1. 1,065 2. 1,14 3. 1,137 4. 1,203 5. 1,014 6. 1,079 7. 0,897 8. 0,909 9. 1,009	0,882

	6. Check the origin and the document itself on reliability 7. Be on your guard when giving personal information to others 8. Reduce internet usage 9. Reducing or stopping certain activities e.g. online banking, downloading...				
Malware_Perceived_severity	To what extent do you agree with the following statements? 1. I think malware is an important problem 2. I think malware should be taken seriously 3. I think malware is a severe problem	5 point likert scale (totally disagree – totally agree)	1. 4,33 2. 4,47 3. 4,27	1. 0,709 2. 0,630 3. 0,761	0,871
Malware_Perceived_vulnerability	To what extent do you agree with the following statements? 1. It is possible that I become a victim of malware 2. It is probable that I become a victim of malware 3. The risk is big that I become a victim of malware	5 point likert scale (totally disagree – totally agree)	1. 3,80 2. 3,21 3. 2,97	1. 0,804 2. 0,914 3. 1,008	0,832
Malware_Self_efficacy	To what extent do you agree with the following statements? 1. Taking the necessary security measures against malware is easy 2. I feel comfortable taking security measures against malware 3. I possess the knowledge and skills to take the necessary security measures against malware	5 point likert scale (totally disagree – totally agree)	1. 3,06 2. 3,49 3. 2,90	1. 0,965 2. 0,946 3. 1,101	0,793

Malware_Response_efficacy	To what extent do you agree with the following statements? 1. Safety measures against malware are effective in preventing malware 2. By taking security measures, I can avoid malware 3. I'm less likely to become a victim of malware if I take security measures	5 point likert scale (totally disagree – totally agree)	1. 3,47 2. 3,61 3. 3,74	1. 0,802 2. 0,813 3. 0,825	0,715
Malware_Attitude	To what extent do you agree with the following statements? 1. Taking security measures against malware is a good idea 2. I love the idea of taking anti-malware measures 3. Taking security measures against malware is important	5 point likert scale (totally disagree – totally agree)	1. 4,18 2. 3,74 3. 4,14	1. 0,673 2. 0,805 3. 0,695	0,827
Malware_Subjective_norm	To what extent do you agree with the following statements? 1. My friends think that I should protect myself from malware 2. People I look up to think that I should protect myself from malware 3. People with whom I compare myself think that I should protect myself from malware	5 point likert scale (totally disagree – totally agree)	1. 2,93 2. 2,82 3. 2,84	1. 0,930 2. 0,891 3. 0,886	0,927
Malware_Intention	To what extent do you agree with the following statements? 1. I'm probably going to take (more) security measures against malware 2. I'm sure I'm going to take (more) security measures against malware	5 point likert scale (totally disagree – totally agree)	1. 3,17 2. 3,03 3. 3,32	1. 0,827 2. 0,831 3. 0,809	0,897

	3. It's possible that I'm going to take (more) security measures against malware				
Scams_Perceived_severity	To what extent do you agree with the following statements? 1. I think Scams are an important problem 2. I think Scams should be taken seriously 3. I think Scams are a severe problem	5 point likert scale (totally disagree – totally agree)	1. 4,35 2. 4,52 3. 4,37	1. 0,707 2. 0,602 3. 0,750	0,888
Scams_Perceived_vulnerability	To what extent do you agree with the following statements? 1. It is possible that I become a victim of Scams 2. It is probable that I become a victim of Scams 3. The risk is big that I become a victim of Scams	5 point likert scale (totally disagree – totally agree)	1. 3,13 2. 2,64 3. 2,46	1. 1,066 2. 1,015 3. 1,054	0,903
Scams_Self_efficacy	To what extent do you agree with the following statements? 1. Taking the necessary security measures against Scams is easy 2. I feel comfortable taking security measures against Scams 3. I possess the knowledge and skills to take the necessary security measures against Scams	5 point likert scale (totally disagree – totally agree)	1. 3,05 2. 3,50 3. 3,14	4. 1,018 5. 0,937 6. 1,108	0,781
Scams_Response_efficacy	To what extent do you agree with the following statements? 1. Safety measures against Scams are effective in preventing Scams 2. By taking security measures, I can avoid Scams	5 point likert scale (totally disagree – totally agree)	1. 3,43 2. 3,56 3. 3,61	1. 0,935 2. 0,929 3. 0,905	0,769

	3. I'm less likely to become a victim of Scams if I take security measures				
Scams_Attitude	To what extent do you agree with the following statements? 1. Taking security measures against Scams is a good idea 2. I love the idea of taking anti-Scams measures 3. Taking security measures against Scams is important	5 point likert scale (totally disagree – totally agree)	1. 4,06 2. 3,67 3. 4,03	1. 0,721 2. 0,825 3. 0,768	0,842
Scams_Subjective_norm	To what extent do you agree with the following statements? 1. My friends think that I should protect myself from Scams 2. People I look up to think that I should protect myself from Scams 3. People with whom I compare myself think that I should protect myself from Scams	5 point likert scale (totally disagree – totally agree)	1. 2,87 2. 2,79 3. 2,80	1. 0,939 2. 0,921 3. 0,913	0,948
Scams_Intention	To what extent do you agree with the following statements? 1. I'm probably going to take (more) security measures against Scams 2. I'm sure I'm going to take (more) security measures against Scams 3. It's possible that I'm going to take (more) security measures against Scams	5 point likert scale (totally disagree – totally agree)	1. 3,09 2. 3,00 3. 3,22	1. 0,872 2. 0,887 3. 0,881	0,918
Hacking_Perceived_severity	To what extent do you agree with the following statements? 1. I think Hacking is an important problem 2. I think Hacking should be taken seriously 3. I think Hacking is a severe problem	5 point likert scale (totally disagree – totally agree)	1. 4,39 2. 4,50 3. 4,41	1. 0,663 2. 0,579 3. 0,692	0,909

Hacking_Perceived_vulnerability	To what extent do you agree with the following statements? 1. It is possible that I become a victim of Hacking 2. It is probable that I become a victim of Hacking 3. The risk is big that I become a victim of Hacking	5 point likert scale (totally disagree – totally agree)	1. 3,73 2. 3,21 3. 3,01	1. 0,828 2. 0,930 3. 1,019	0,863
Monitoring_Perceived_severity	To what extent do you agree with the following statements? 1. I think Monitoring is an important problem 2. I think Monitoring should be taken seriously 3. I think Monitoring is a severe problem	5 point likert scale (totally disagree – totally agree)	1. 3,76 2. 4,02 3. 3,68	1. 1,000 2. 0,838 3. 1,043	0,911
Monitoring_Perceived_vulnerability	To what extent do you agree with the following statements? 1. It is possible that I become a victim of Monitoring 2. It is probable that I become a victim of Monitoring 3. The risk is big that I become a victim of Monitoring	5 point likert scale (totally disagree – totally agree)	1. 3,65 2. 3,39 3. 3,27	1. 0,986 2. 1,030 3. 1,096	0,931
Cybercrime_Self_efficacy	To what extent do you agree with the following statements? 1. Taking the necessary security measures against Cybercrime is easy 2. I feel comfortable taking security measures against Cybercrime 3. I possess the knowledge and skills to take the necessary security measures against Cybercrime	5 point likert scale (totally disagree – totally agree)	1. 2,69 2. 3,34 3. 2,64	1. 0,986 2. 0,994 3. 1,089	0,736

Cybercrime_Response_efficacy	To what extent do you agree with the following statements? 1. Safety measures against Cybercrime are effective in preventing Cybercrime 2. By taking security measures, I can avoid Cybercrime 3. I'm less likely to become a victim of Cybercrime if I take security measures	5 point likert scale (totally disagree – totally agree)	1. 3,27 2. 3,37 3. 3,82	1. 0,870 2. 0,937 3. 0,819	0,659*
Cybercrime_Attitude	To what extent do you agree with the following statements? 1. Taking security measures against Cybercrime is a good idea 2. I love the idea of taking anti-Cybercrime measures 3. Taking security measures against Cybercrime is important	5 point likert scale (totally disagree – totally agree)	1. 4,28 2. 3,81 3. 4,26	1. 0,692 2. 0,830 3. 0,678	0,798
Cybercrime_Subjective_norm	To what extent do you agree with the following statements? 1. My friends think that I should protect myself from Cybercrime 2. People I look up to think that I should protect myself from Cybercrime 3. People with whom I compare myself think that I should protect myself from Cybercrime	5 point likert scale (totally disagree – totally agree)	1. 2,92 2. 2,83 3. 2,83	1. 0,942 2. 0,884 3. 0,876	0,871
Cybercrime_Intention	To what extent do you agree with the following statements? 1. I'm probably going to take (more) security measures against Cybercrime 2. I'm sure I'm going to take (more) security measures against Cybercrime	5 point likert scale (totally disagree – totally agree)	1. 3,18 2. 3,07 3. 3,40	1. 0,803 2. 0,809 3. 0,788	0,871

	3. It's possible that I'm going to take (more) security measures against Cybercrime				
Victimization	Have you, or anyone else in your family fell victim of any of the following phenomenon's in the past 12 months 1. Malware 2. Scams 3. Hacking 4. Monitoring	Yes, myself Yes, someone else in my family Yes, both me and someone else in my family I guess so No I don't know			
Malware_frequency (n=216)	In the last 12 months, how many times did y(our) family fell victim to Malware?	Once, Twice, Three times, Four times, Five times or more, I don't know	3,64	2,313	
Malware_report	Did you report this incident (multiple answers possible)	Yes, to the police Yes, to the internet provider Yes, to another body No			
Malware_defence_cost (n=246)	How much do you estimate you spend to defend you(r family) against malware last year? (e.g. €10).	Open question + "I don't know"	€61,99	€43,16	
Malware_direct_monetary_cost (n=198)	How big were the financial consequences of malware the last 12 months? Think about costs linked to damage, repair, ransom. Give the answer in € (e.g. €10)	Open question	€108,37	€839,07	
Malware_direct_non-monetary_cost (n=193)	Indicate how harmful you estimate the malware incident for you (r family) in terms of different components. Choose the appropriate answer for each item. When assessing the severity of the damage, please use the following criterion:	Harmless Insignificant Moderate Serious Grave Catastrophic Does not apply	1. 2,83 2. 2,33 3. 2,82	1. 1,369 2. 1,400 3. 1,570	0,886

	catastrophic damage could mean that you can no longer perform a particular component for more than 6 months (e.g. performing daily operations, protecting reputation, ensuring privacy). insignificant means that you cannot do a particular part for a short while. harmless means that this incident does not affect the questioned. does not apply means that this incident cannot affect the component. 1. Daily actions 2. Reputation 3. Privacy				
Scams_frequency **(n=92)**	In the last 12 months, how many times did y(our) family fell victim to Scams?	Once, Twice, Three times, Four times, Five times or more, I don’t know	2,70	2,170	
Scams_report	Did you report this incident (multiple answers possible)	Yes, to the police Yes, to the banc/financial body Yes, to the consumer organisation Yes, to another body No			
Scams_defence_cost **(n=73)**	How much do you estimate you spend to defend you(r family) against Scams last year? (e.g. €10).	Open question + “I don’t know”	€51,40	€34,94	
Scams_direct_monetary_cost **(n=90)**	How big were the financial consequences of Scams the last 12 months? Think about costs linked to damage, repair, ransom. Give the answer in € (e.g. €10)	Open question	€12286,77	€99105,64	

Scams_direct_non-monetary_cost (n=73)	Indicate how harmful you estimate the Scams incident for you (r family) in terms of different components. Choose the appropriate answer for each item. When assessing the severity of the damage, please use the following criterion: catastrophic damage could mean that you can no longer perform a particular component for more than 6 months (e.g. performing daily operations, protecting reputation, ensuring privacy). insignificant means that you cannot do a particular part for a short while. harmless means that this incident does not affect the questioned. does not apply means that this incident cannot affect the component. 1. Daily actions 2. Reputation 3. Privacy	Harmless Insignificant Moderate Serious Grave Catastrophic Does not apply	1. 2,74 2. 2,51 3. 2,71	1. 1,558 2. 1,465 3. 1,628	0,915
Hacking_frequency (n=120)	In the last 12 months, how many times did y(our) family fell victim to Hacking?	Once, Twice, Three times, Four times, Five times or more, I don't know	3,27	2,37	
Hacking_report	Did you report this incident (multiple answers possible)	Yes, to the police Yes, to the internet provider Yes, to the company of which the account was hacked Yes, to another body No			
Hacking_defence_cost (n=137)	How much do you estimate you spend to defend you(r family) against Hacking last year? (e.g. €10).	Open question + "I don't know"	€62,75	€92,39	

Hacking_direct_monetary_cost (n=111)	How big were the financial consequences of Hacking the last 12 months? Think about costs linked to damage, repair, ransom. Give the answer in € (e.g. €10)	Open question	€109,97	€953,81	
Hacking_direct_non-monetary_cost (n=99)	Indicate how harmful you estimate the Hacking incident for you (r family) in terms of different components. Choose the appropriate answer for each item. When assessing the severity of the damage, please use the following criterion: catastrophic damage could mean that you can no longer perform a particular component for more than 6 months (e.g. performing daily operations, protecting reputation, ensuring privacy). insignificant means that you cannot do a particular part for a short while. harmless means that this incident does not affect the questioned. does not apply means that this incident cannot affect the component. 1. Daily actions 2. Reputation 3. Privacy	Harmless Insignificant Moderate Serious Grave Catastrophic Does not apply	1. 2,96 2. 2,61 3. 3,05	1. 1,584 2. 1,480 3. 1,632	0,872
Monitoring_frequency (n=161)	In the last 12 months, how many times did y(our) family fell victim to Monitoring?	Once, Twice, Three times, Four times, Five times or more, I don't know	5,69	1,025	
Monitoring_report	Did you report this incident (multiple answers possible)	Yes, to the police Yes, to the internet provider Yes, government Yes to another body			

		No			
Monitoring_defence_cost **(n=53)**	How much do you estimate you spend to defend you(r family) against Monitoring last year? (e.g. €10).	Open question + “I don’t know”	€53,48	€70,51	
Monitoring_direct_monetary_cost **(n=144)**	How big were the financial consequences of Monitoring the last 12 months? Think about costs linked to damage, repair, ransom. Give the answer in € (e.g. €10)	Open question	€9621,49	€97551,28	
Monitoring_direct_non-monetary_cost **(n=133)**	Indicate how harmful you estimate the Monitoring incident for you (r family) in terms of different components. Choose the appropriate answer for each item. When assessing the severity of the damage, please use the following criterion: catastrophic damage could mean that you can no longer perform a particular component for more than 6 months (e.g. performing daily operations, protecting reputation, ensuring privacy). insignificant means that you cannot do a particular part for a short while. harmless means that this incident does not affect the questioned. does not apply means that this incident cannot affect the component. 1. Daily actions 2. Reputation 3. Privacy	Harmless Insignificant Moderate Serious Grave Catastrophic Does not apply	1. 2,21 2. 2,30 3. 3,26	1. 1,372 2. 1,364 3. 1,699	0,841
cybercrime_opportunity_costs	To what extent do you agree with the statements below?	5 point Likert (totally disagree – totally agree	1. 1,83 2. 2,05 3. 1,98	1. 0,911 2. 1,045 3. 1,025	0,832

	1. Due to concerns about the safety of the Internet, I have done online banking less often or no longer the last 12 months. 2. Due to concerns about the safety of the Internet, I have done online shopping less often or no longer the last 12 months. 3. Due to concerns about the safety of the Internet, I have used social networks less often or no longer the last 12 months.	+ I didn't do this in the first place)			
Cybercrime_defence_cost (n=263)	How much do you estimate you spend to defend you(r family) against all cybercrimes (malware, scams, hacking and monitoring) last year? (e.g. €10).	Open question + "I don't know"	€67,72	€67,60	
Security_measures_taken	Do you take one or more of the following security measures to defend you(r family) against such phenomena (malware, scams, hacking, monitoring) (multiple answers possible) 1. Install free software e.g. anti-virus program, anti-spyware, anti-phishing crypto, backup software 2. Install paying software e.g. anti-virus program, anti-spyware, anti-phishing crypto, backup software 3. Set up software provided by operating system (e.g. firewall, defender) 4. Update software and operating systems 5. Secure Wi-Fi network 6. Use hard-to-guess passwords for accounts and home network 7. Check senders and documents for reliability	Malware Scams Hacking Monitoring I don't do this			

	8. Be on guard when giving personal information to third party 9. Reduce Internet usage 10. Avoid or stop certain activities online e.g. online banking, downloading ...				

For certain constructs, the sample size of that question is added to the construct. This is because in those constructs were asked at a certain type of respondent (e.g. victims of malware…) or there was an option to answer “I don’t know”, “I don’t do this” or “I don’t pay any money”. Because these answers would influence the means and standard deviations enormously these were not included in the calculations. It is, however, important to note that these values are talking about a part of the total sample.

*because of the theoretical value of response efficacy of cybercrime in general there is chosen to keep this construct even if the Cronbach’s Alpha is not above the 0,7 threshold.

Appendix B: PCA all cybercrimes

	M	SD	Factor Loading (CFA)
Threat awareness*	3,455	0,98323	
TA1			.573
TA2			.867
TA3			.916
Coping awareness**	3,6326	0,83977	
CA1			0,83
CA2			0,839
CA3			0,843
CA4			0,781
CA5			0,71
CA6			0,637
CA7			0,539
Perceived Severity	4,3955	0,5113	
PS_Malware			0,673
PS_Scam			0,688
PS_Hack			0,822
Perceived Vulnerability	3,1372	0,7046	
PS_Malware			0,713
PS_Scam			0,646
PS_Hack			0,827
Self-efficacy	2,9	0,82307	
SE1			0,681
SE2			0,63
SE3			0,78
Response efficace	3,4894	0,67662	
RE1			0,67
RE2			0,675
RE3			0,559
Attitude towards behaviour	4,1126	0,62105	
ATT1			0,86
ATT2			0,596
ATT3			0,862

Social Norm	2,8657	0,80816	
SN1			0,684
SN2			0,906
SN3			0,923
Intention towards behaviour	3,2196	0,71673	
INT1			0,933
INT2			0,833
INT3			0,745

*Monitoring is not included as a cybercrime

**Only adaptive security measures are included in the SEM model

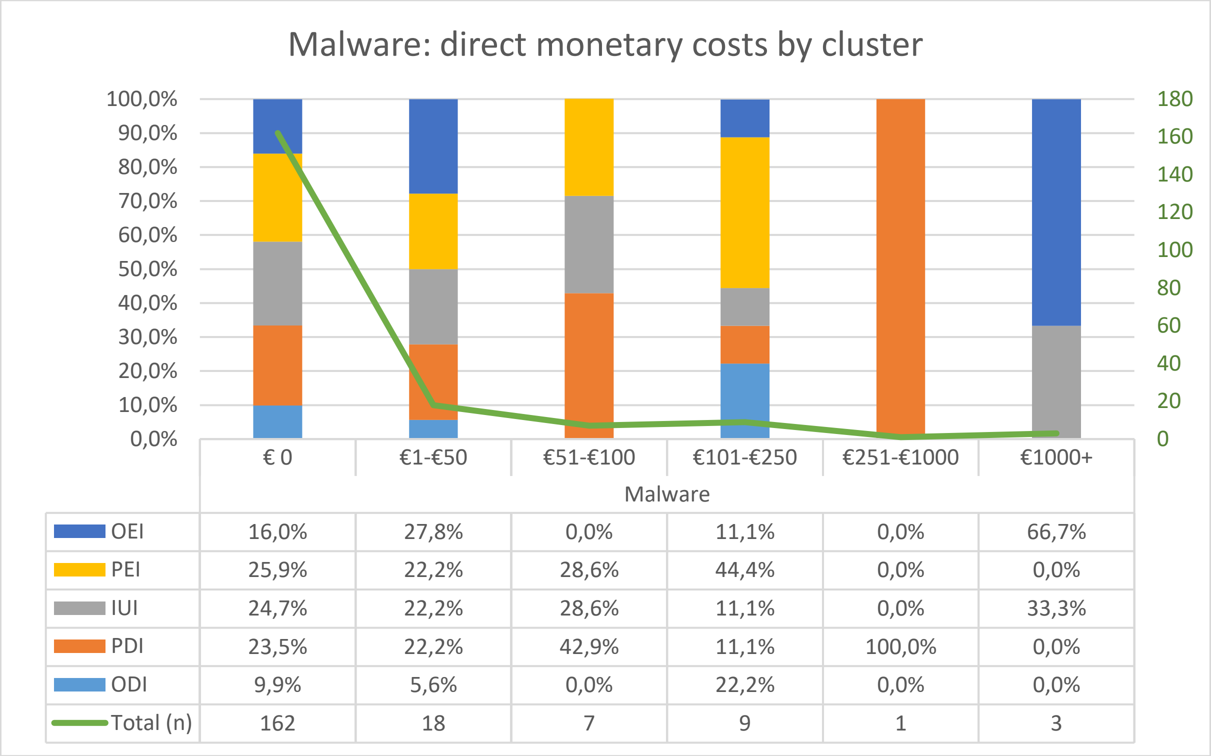
Appendix C: PCA Malware

	M	SD	Factor Loading (CFA)
Malware awareness	3,02	1,361	n.a.
Coping awareness	3,6326	0,83977	
CA1			0,837
CA2			0,85
CA3			0,857
CA4			0,781
CA5			0,702
CA6			0,634
CA7			0,533
Perceived Severity Malware	4,3494	0,63381	
PS_Malware_1			0,881
PS_Malware_2			0,774
PS_Malware_3			0,854
Perceived Vulnerability Malware	3,3345	0,78149	
PV_Malware_1			0,673
PV_Malware_2			0,923
PV_Malware_3			0,8
Self-efficacy Malware	3,1547	0,84716	
SE_Malware_1			0,76
SE_Malware_2			0,654
SE_Malware_3			0,847
Response efficace Malware	3,6142	0,6546	
RE_Malware_1			0,752
RE_Malware_2			0,733
RE_Malware_3			0,566
Attitude towards behaviour Malware	4,0192	0,62753	
ATT_Malware_1			0,881
ATT_Malware_2			0,618
ATT_Malware_3			0,914
Social Norm	2,8747	0,84801	
SN_Malware_1			0,813
SN_Malware_2			0,942
SN_Malware_3			0,949
Intention towards behaviour Malware	3,1668	0,75684	
INT_Malware_1			0,937
INT_Malware_2			0,836
INT_Malware_3			0,83

Appendix D: PCA Scams

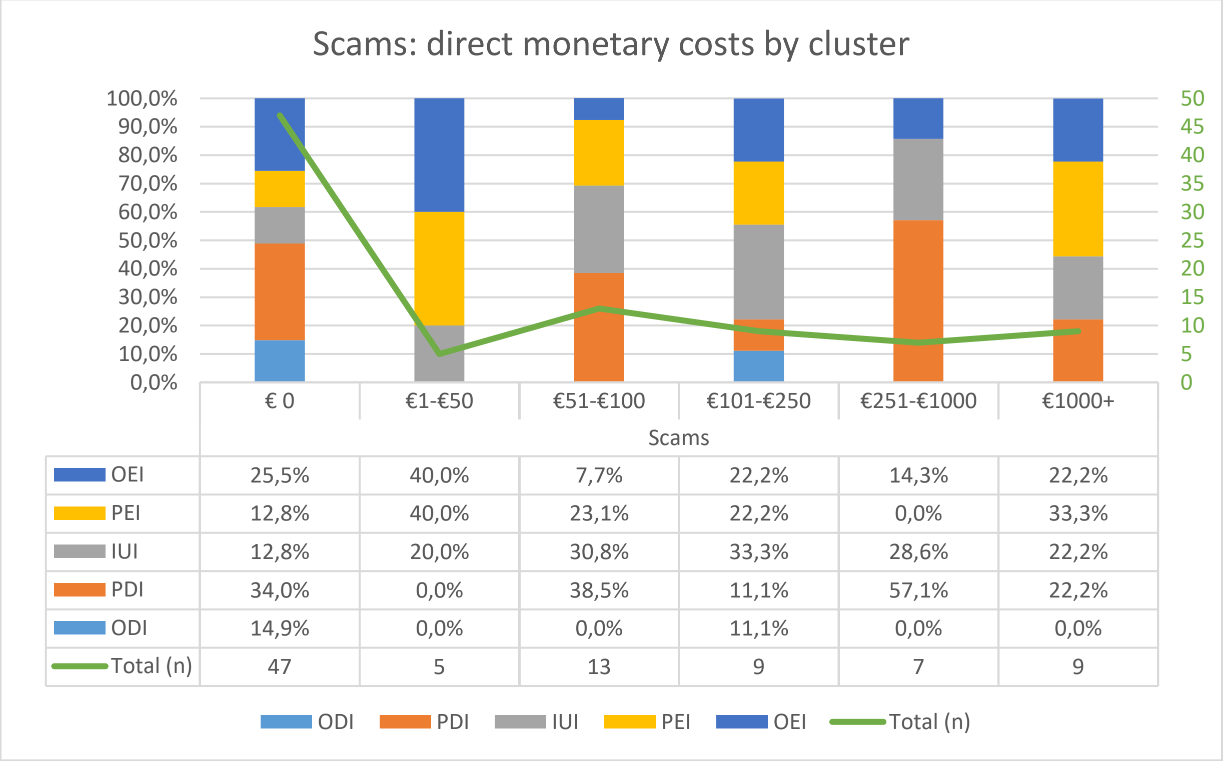
	M	SD	Factor Loading (CFA)
Scam awareness	3,72	1,062	n.a.
Coping awareness	3,6326	0,83977	
CA1			0,833
CA2			0,839
CA3			0,844
CA4			0,776
CA5			0,712
CA6			0,633
CA7			0,54
Perceived Severity Scam	4,4093	0,6287	
PS_Scam_1			0,851
PS_Scam_2			0,835
PS_Scam_3			0,884
Perceived Vulnerability Scam	2,7536	0,95598	
PV_Scam_1			0,764
PV_Scam_2			0,973
PV_Scam_3			0,89
Self-efficacy Scam	3,2297	0,85044	
SE_Scam_1			0,778
SE_Scam_2			0,661
SE_Scam_3			0,776
Response efficace Scam	3,534	0,76684	
RE_Scam_1			0,757
RE_Scam_2			0,801
RE_Scam_3			0,652
Attitude towards behaviour Scam	3,9181	0,67723	
ATT_Scam_1			0,886
ATT_Scam_2			0,665
ATT_Scam_3			0,894
Social Norm	2,8335	0,88038	
SN_Scam_1			0,863
SN_Scam_2			0,953
SN_Scam_3			0,963
Intention towards behaviour Scam	3,107	0,81945	
INT_Scam_1			0,948
INT_Scam_2			0,885
INT_Scam_3			0,844

Appendix E: Detailed overview of direct monetary costs per cluster



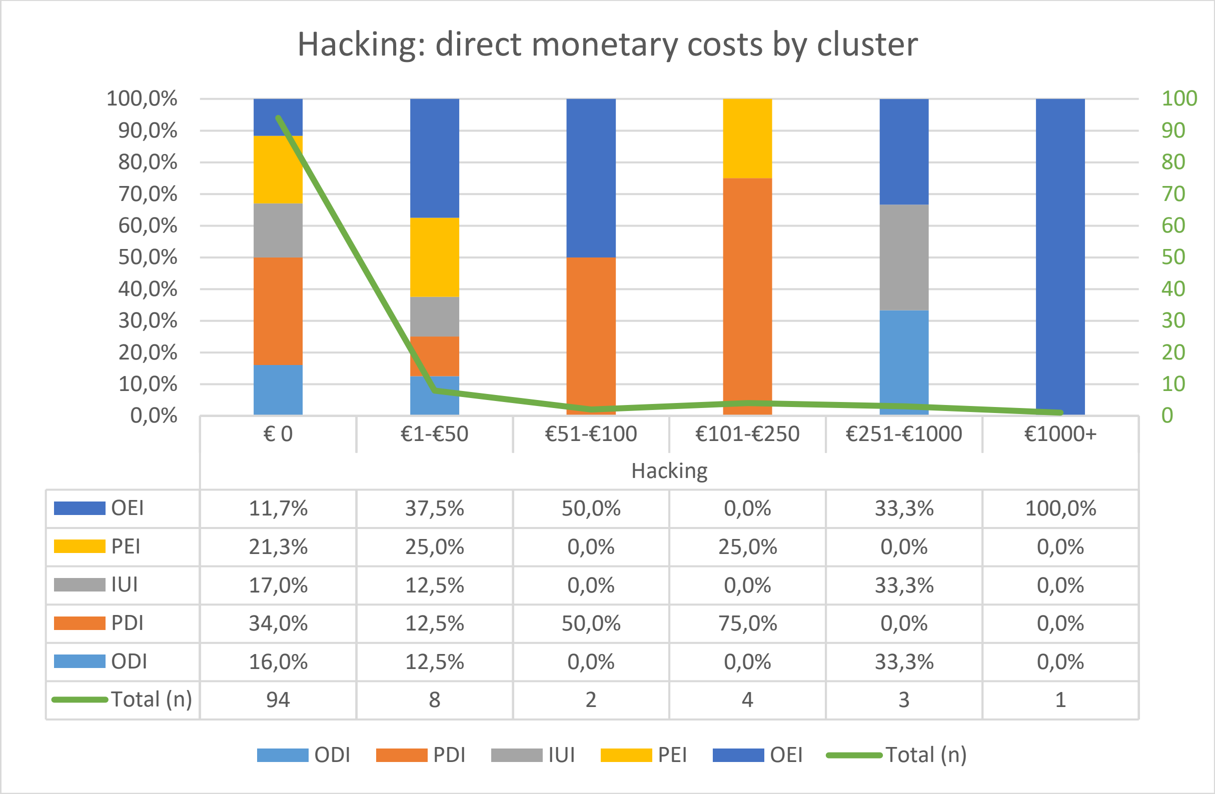
Malware: direct monetary costs by cluster

Malware	€ 0	€1-€50	€51-€100	€101-€250	€251-€1000	€1000+
OEI	16,0%	27,8%	0,0%	11,1%	0,0%	66,7%
PEI	25,9%	22,2%	28,6%	44,4%	0,0%	0,0%
IUI	24,7%	22,2%	28,6%	11,1%	0,0%	33,3%
PDI	23,5%	22,2%	42,9%	11,1%	100,0%	0,0%
ODI	9,9%	5,6%	0,0%	22,2%	0,0%	0,0%
Total (n)	162	18	7	9	1	3



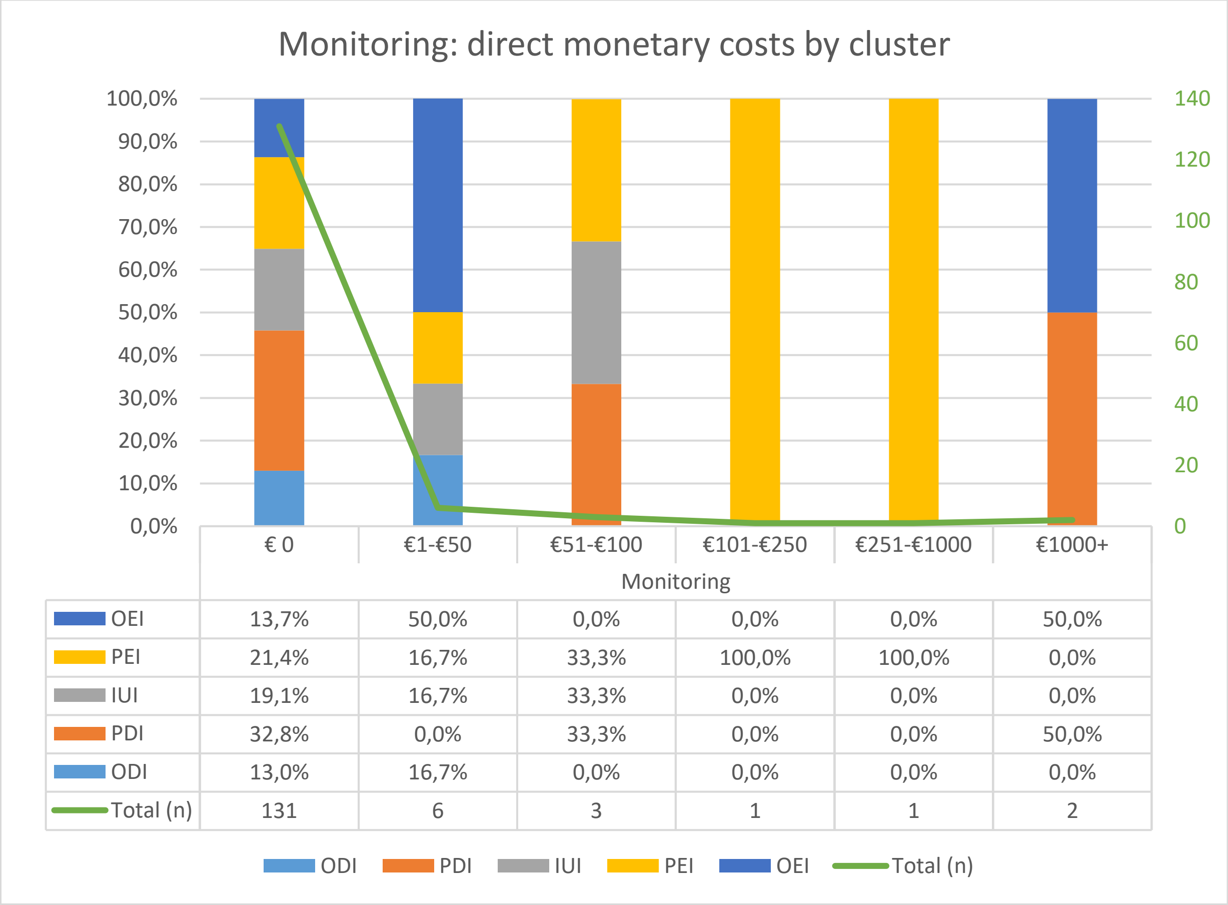
Scams: direct monetary costs by cluster

Scams	€ 0	€1-€50	€51-€100	€101-€250	€251-€1000	€1000+
OEI	25,5%	40,0%	7,7%	22,2%	14,3%	22,2%
PEI	12,8%	40,0%	23,1%	22,2%	0,0%	33,3%
IUI	12,8%	20,0%	30,8%	33,3%	28,6%	22,2%
PDI	34,0%	0,0%	38,5%	11,1%	57,1%	22,2%
ODI	14,9%	0,0%	0,0%	11,1%	0,0%	0,0%
Total (n)	47	5	13	9	7	9



Hacking: direct monetary costs by cluster

	€ 0	€1-€50	€51-€100	€101-€250	€251-€1000	€1000+
OEI	11,7%	37,5%	50,0%	0,0%	33,3%	100,0%
PEI	21,3%	25,0%	0,0%	25,0%	0,0%	0,0%
IUI	17,0%	12,5%	0,0%	0,0%	33,3%	0,0%
PDI	34,0%	12,5%	50,0%	75,0%	0,0%	0,0%
ODI	16,0%	12,5%	0,0%	0,0%	33,3%	0,0%
Total (n)	94	8	2	4	3	1



Monitoring: direct monetary costs by cluster

	€ 0	€1-€50	€51-€100	€101-€250	€251-€1000	€1000+
OEI	13,7%	50,0%	0,0%	0,0%	0,0%	50,0%
PEI	21,4%	16,7%	33,3%	100,0%	100,0%	0,0%
IUI	19,1%	16,7%	33,3%	0,0%	0,0%	0,0%
PDI	32,8%	0,0%	33,3%	0,0%	0,0%	50,0%
ODI	13,0%	16,7%	0,0%	0,0%	0,0%	0,0%
Total (n)	131	6	3	1	1	2