Martínez de Ibarreta, Carlos; Gijón, Covadonga

Conference Paper

Cybersecurity and risk behaviour on mobile individual consumers in Spain

27th European Regional Conference of the International Telecommunications Society (ITS): "The Evolution of the North-South Telecommunications Divide: The Role for Europe", Cambridge, United Kingdom, 7th-9th September, 2016

Provided in Cooperation with:

International Telecommunications Society (ITS)

Suggested Citation: Martínez de Ibarreta, Carlos; Gijón, Covadonga (2016) : Cybersecurity and risk behaviour on mobile individual consumers in Spain, 27th European Regional Conference of the International Telecommunications Society (ITS): "The Evolution of the North-South Telecommunications Divide: The Role for Europe", Cambridge, United Kingdom, 7th-9th September, 2016, International Telecommunications Society (ITS), Calgary

This Version is available at:
https://hdl.handle.net/10419/148690

Cybersecurity and risk behaviour on mobile individual consumers in Spain

Carlos Martínez de Ibarreta,
Universidad Pontificia de Comillas (ICADE), Spain
charlie@cee.upcomillas.es

Covadonga Gijón,
Universidad Carlos III de Madrid, Spain
mgijon@eco.uc3m.es

Abstract

Nowadays a big and increasing proportion of world's population uses Internet in their day life and web connection via mobile is having a growing importance. Day by day there is more information about the risks and dangers of a misuse of Internet and mobile phones, which may involve all sorts of negative consequences, from computer malfunction to economical or personal damages.

Almost 30% of Spanish mobile users acknowledge to have suffered any kind of mobile security incident during the last three months, whereas roughly 20% of them acknowledge to have suffered any kind of fraud via mobile. Consequently, a significant fraction of users has been victim of some kind of cyber-attacks.

In this paper it is observed, among others, positive relationship between level of security measures and level of attacks or frauds. There are two possibilities: the risk compensation theory or protection after an attack or fraud.

Keywords: *cybersecurity, mobile, cyber-attacks, fraud, behaviour*

1. Introduction

Nowadays a big and increasing proportion of world's population uses Internet in their day life and web connection via mobile is having a growing importance. At global world level there is empirical evidence that mobile Internet access have overtaken fixed Internet access by 2014. This is also the situation in Spain, as is stablished in *La sociedad de la información en España 2015* (Fundación Telefónica, 2016). According to this report, mobile is the main device used to access to the Internet for 88.3% of users, an increase of 5.9 points with respect to 2014.

At the same time number and typology of cyber-attacks is growing ever faster. They include all types of malware, such as viruses, trojans, adware, worms, heuristics, rogue ware, and several forms of online fraud, such as phishing, stealing of passwords or personal information, etc.

Online commerce is growing, and as Buttler (2014) said, the security of this kind of commerce is very important for the organisations, consumers and governments. Educate individuals for using security software and choosing better passwords is one of the most important things in this kind of commerce.

User behaviour has grown significantly. Jin, Chen, Wang, Hui and Vasilakos (2013) focus users' behaviour in online social networks, and they analyse the behaviour in four different perspectives: connection and interaction, traffic activity, mobile social behaviour, and malicious behaviour.

There are lots of protection tools against cyber-attacks. There are some whose operation that can be automated, such as antivirus or firewall, whereas there are others that require an active behaviour from the user, such as deleting cookies or doing backups of crucial files.

All these tools and measures or some of equivalent nature are widely disposable for the smartphones. However, nowadays these tools are less common in mobiles than in computers, due to at the beginning mobile phones had no Internet connexion and many users that migrated from these mobiles to new smartphones did not think that protection measures, such as an antivirus were needed for their mobile devices.

Furthermore, day by day there is more information about the risks and dangers of a misuse of Internet and mobile phones, which may involve all sorts of negative consequences, from computer malfunction to economical or personal damages.

Despite all that, as data shows, almost 30% of Spanish mobile users acknowledge to have suffered any kind of mobile security incident during the last three months, whereas roughly 20% of them acknowledge to have suffered

any kind of fraud via mobile. Consequently, a significant fraction of users has been victim of some kind of cyber-attacks.

The likelihood and frequency of these security incidents (often followed by consequent frauds) are driven, on one hand, by the growing variety and sophistication of mechanisms and tools to make cyber-attacks, but on the other hand for a bad combination of risky behaviour of users while using their mobiles and surfing the Internet and the lack of enough defensive and protective measures in their devices.

This paper tries to give empirical answer about which are the key factors that influence the likelihood of a mobile user has a higher propensity or likelihood to suffer cyber-attacks in his or her mobile phone.

These factors can be grouped into several categories as follows. For each of one some empirically testable hypotheses are proposed.

Regarding the factors that can influence in engaging in risky behaviours while using the Smartphone, that eventually can lead to cyber-attacks and fraud (or fraud attempt) it is possible to distinguish between these two classes:

A. Psychological factors related with age and gender. Psychology and neurosciences show that there is a general law that says that risk preferences decline with age (Paulsen *et al.*, 2013) and they tend to be lower in females than in males (Byrnes *et.al,* 1999). Therefore it can be expected that this law also comply in the Internet behaviour.

B. Education and knowledge about the Internet and its risks. The global hypothesis that it is made is that the more knowledge level one individual has, the lesser the likelihood to engage in risky behaviour that could harm the computer.

This educational dimension can be detailed in several sub dimensions:

B1) Education (in a broad sense). It is supposed that if one individual has achieved a greater education level and he or she also lives in an environment where there are more availability of technological information and resources, such as in a big city, it is less likely that she or he engages into risky behaviour.

> *H1a: There is an inverse relationship between education level and level of mobile attack or fraud suffered*
>
> *H1b: There is an inverse relationship between habitat size and level of mobile attack or fraud suffered*

B2) Knowledge about the Internet and mobile operating reached by means of experience. This expertise can be achieved by tenure or by being familiar with services and applications well known by the user. It is supposed that when an

individual is using a new application or service is easier that he or she makes a risky behaviour, because he or she is not familiar with it and it is easier to make a mistake. Conversely, that is harder when one has enough expertise in using some application.

> *H2a: There is an inverse relationship between Internet experience level and level of mobile attack or fraud suffered*
>
> *H2b: The greater the number and diversity of services and applications used, the greater the likelihood suffer a mobile attack or fraud*

With respect to the relationship between the mobile protection level and the attack/fraud level there are two competing hypothesis.

On the one hand, it is supposed that a mobile user that has installed more protection tools, such as antivirus, or one user that takes intentional security actions such as do backups of relevant information, has greater knowledge level about the Internet and its risks. Therefore there will be lower probability of he or she suffers any attack or fraud.

> *H3: The more cybersecurity level (both active and passive) an individual has, the lower his or her probability to suffer a mobile attack or fraud.*

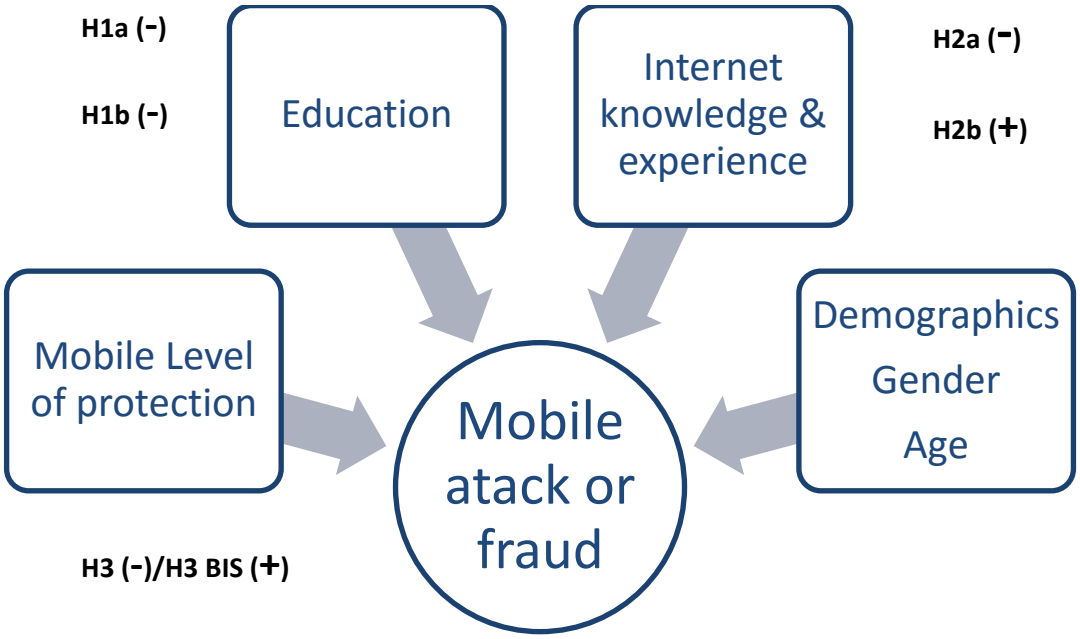
But on the other hand, in this field could be operating the mechanisms described by the risk compensation theory or risk homeostasis theory. Risk homeostasis theory posits that people adjust their behaviours to compensate for factors that raise or lower risk in order to maintain a constant accepted risk level (Wilde, 1998). This theory is most often discussed in safety science literature, for example, to explain why drivers might be more likely to exceed speed limits while wearing seat belts.

Some work (Pearman *et.al*, 2016, Christin *et.al*, 2011) suggests that users are more likely to engage in specific risky behaviours (such as visiting unsafe websites or ignoring security patches) when they believe that they are protected by antivirus software. May be that risk compensation theory is also suitable to mobile phones use. Therefore the following competing hypothesis is set:

> *H3BIS: The more cybersecurity level (both active and passive) an individual has, the higher his or her probability to suffer a mobile attack or fraud.*

Figure 1 outlines a conceptual model with the relationships among these constructs as well the hypothesis established

Figure 1. Conceptual model and hypothesis



The rest of paper is organized as follows, in section 2 there is information about the data, the variables and the models used for the empirical research. Section 3 presents the main empirical results. Finally section 4 concludes.

2. Data, variables, models

2.1 Data

Data used in this paper comes from a survey with data on 3,010 households of Spanish Internet users: Estudio sobre Ciberseguridad y confianza en los hogares españoles (*Study on Cybersecurity and Trust in Spanish households*). The data was collected from December of 2013 to January 2014, by Instituto Nacional de Tecnologías de la Comunicación (INTECO) and Observatorio Nacional de las Telecomunicaciones y de la Sociedad de la Información (ONTSI), which are government body that performs, among other functions, the collection and analysis of socio-economic data. The survey is about households that have Internet connection and includes questions about socio-demographics, different kinds of security, Internet use, mobile use behaviour on Internet use, security incidences, phishing, etc.

Table 1 presents the demographic profile of the respondents to the survey (calculus are referred to estimation sample (n=2118) instead to the whole sample n=3010). The survey is about the household but the profile is the person that answered the survey. It can be seen that the majority of respondents are

older than 35, with more than half of them being between 35 and 54 years old. The sample is representative of the Spanish population of Internet users.

Table 1. Demographic profile of respondent (estimation sample size 2118)

		Frequency	*Percent*
Gender	Male	1,145	54.06
	Female	973	45.94
Age	15-24	147	6.94
	25-34	489	23.09
	35-44	793	37.44
	45-54	465	21.95
	>55	224	10.58
Habitat size	<10k	256	12.09
	10-50k	455	21.48
	50-100k	196	9.25
	>100k	252	11.90
	Capital <500k	401	18.93
	Capital >500k	558	26.35
Education level	Primary	23	1.09
	High School	986	46.55
	College	1109	52.36
Time being Internet user	<1 year	12	0.57
	2 – 5 years	89	4.20
	< 5 years	2,017	95.23
Intensity of Internet use	At least once a day	2,030	95.85
	At least once a week	77	3.64
	At least once a month	9	0.42
	Less than once a month	2	0.09

More than half of the sample lives in capital cities or cities with a population over 100.000 habitants. Also more than 50% of the respondents have education at a graduate level.

2.2. Models

To test the hypothesis proposed in previous section, and to improve robustness of results, some different models have been specified, depending on how the dependent variable has been defined and measured.

Both concepts of “mobile security attack” and “mobile fraud” have been computed as:

a) A composite index built as the first principal component of a principal component analysis (PCA) made over the binary indicators in the survey related with each of the constructs. Details about these indexes are shown in the next subsection. In this case, as these indexes are of numerical nature, standard linear regression models have been estimated.

b) A binary variable indicating if the user has suffered or not any security attack or any mobile fraud during the last three months. In this case binary logit models have been estimated
c) A count variable capturing how many security incidents or how many mobile frauds a user has suffered during the previous three months. In this case, count models, as Poisson regression or Negative Binomial regression have been employed. The second one would be preferred in the case of over-dispersion (due to a contagion effect in the count of the dependent variable)

The explanatory variables, following the conceptual model are grouped into the following three vectors of variables: socio-demographics (SD), Internet and mobile use patterns (I), and mobile security measures (MS)

Therefore in the case a) the models can be expressed as is shown in equation [1]:

$$security\ attack\ (fraud)index = \alpha + \boldsymbol{SD\beta} + \boldsymbol{I\gamma} + \boldsymbol{MS\delta} + \varepsilon \qquad [1]$$

In the case b) the models become as shown in equation [2]

$$prob(attack = 1) = \frac{e^z}{1+e^z} \qquad z = \alpha + \boldsymbol{SD\beta} + \boldsymbol{I\gamma} + \boldsymbol{MS\delta} + \varepsilon \qquad [2]$$

Finally in the case c) the model equation (for the case of Poisson regression) is as presented in equation [3]

$$prob(number\ of attacks = x) = \frac{e^{-\lambda}\lambda^x}{x!} \qquad \lambda = \alpha + \boldsymbol{SD\beta} + \boldsymbol{I\gamma} + \boldsymbol{MS\delta} + \varepsilon \qquad [3]$$

Negative binomial regression model will be preferred when the test for overdispersion rejects the null hypothesis (i.e. if variance of dependent variable greater than its mean). As the Poisson regression is a restricted version of the Negative Binomial regression, the strategy to choose between the two types of models is to estimate first the negative binomial model and then perform the overdispersion test. If the null is not rejected then the Poisson regression will be estimated.
In order to prevent inference errors derived from heteroskedasticity, robust standard errors have been used in all the models to prevent inference errors derived from that problem.

2.3. Variables definition

This subsection is devoted to explain the definition of the sets of variables mentioned above, that is, the security attack and the level of fraud indexes, the Internet use patterns (I) and the mobile security measures (MS)

Each of the variables labelled as “indexes” are built as the scores of the first principal component resulting from a principal components analysis (PCA). In each of the PCA performed, it has been employed as original variables those indicators (mainly of a binary nature) which appear in the questionnaire and related with the corresponding construct. Table 2 details the indicators that form each of the indexes, as well the percentage of users in each of the indicators with value one.

A) Dependent variables: mobile security attack index and level of fraud index

- *Security attack index.* The higher its value the greater the level of mobile security attacks suffered by the user. It has been built as the first component of a principal component analysis (PCA) made over the binary indicators in the survey related with security attacks. From table 2 it can be seen that the most frequent security pitfall is to receive undesired mobile spam (22%), followed by having a wrong bill (5%). Almost 30% of users have suffered any kind of incident during the last three months
- *Number of security attacks*. Table 3 shows the frequency distribution of number of mobile security attacks suffered by each user during the last three months. It can be seen that although 71% of users did not suffered any kind of incident, 24% suffered one and 4% more than one. As the mean and the variance are almost identical, overdispersion test fails to reject the null hypothesis and Poisson regression is the count model estimated in this case.
- *Level of fraud suffered index*. The higher its value the greater the level of mobile frauds suffered by the user. It has been built as the first component of a principal component analysis (PCA) made over the binary indicators in the survey related with mobile frauds. From table 2 it can be seen that the most frequent mobile frauds are receiving calls or messages with suspicious business deals to be fraudulent (9%) and receiving requests to open a file or a suspicious web link (7%). Almost 21% of users have suffered (or have near to suffer) any kind of fraud during the last three months. The lineal correlation between this index and the security attack index is 0.44

- *Number of frauds suffered*. Table 4 shows the frequency distribution of number of mobile frauds (or fraud attempts) suffered by each user during the last three months. It can be seen that although 80% of users did not suffered any kind of incident, 14% suffered one and 6% more than one. As the the variance is clearly greater then mean, overdispersion test reject the null hypothesis and Negative binomial regression is the count model estimated in this case. The lineal correlation between number of attacks and number of frauds is 0.49.

B) Internet and mobile use patterns

- *Time being Internet user.* It is a recency measure that takes values 1 to 3 depending on the users’ answers to the item in the questionnaire labelled:

how long are you using the Internet? Value 1 corresponds to the answer "less than a year", value 2 to "between one and 5 years", whereas value 3 corresponds to the answer "more than 5 years".

- *Intensity of Internet use*. It is a frequency measure that takes values 1 to 4 depending on the users' answers to the item in the questionnaire labelled: *how often do you connect to the Internet at home?* Value 1 corresponds to the answer "less than once at a month", whereas value 4 corresponds to the answer "at least once a day".
- *Diversity Mobile Use Index*. The higher its value, the greater the number of mobile applications, programs and services used by the individual in the last three months in his or her smartphone. From Table 2 it can be highlighted than the services more often used are e-mail (78%), social networks (69%) and games through mobile (46%).

C) Mobile security measures

- *Mobile Security Measures Index*. The higher its value the greater the number of protection tools and security measures than the individual has implemented in his or her smartphone. Some of these measures, such as using passwords, or doing periodic backups require an active behaviour from user because they cannot be automated, whereas others, as having an antivirus installed are of more passive nature and can be automated. The most often employed security measures are using passwords (59%) and doing backups of contacts and other kind of data and files (pictures, documents…). As mentioned in the introduction, the level of implementation of tools and security measures is much lower in mobile devices than in computers. For instance, only 32% of users have installed an antivirus in their mobile in comparison with 82% of users that have it installed in their desktop computers or laptops.
- *Having installed or not an antivirus*. Due to its importance alone as a protection tool, all the models have been alternatively estimated using this dichotomous variable instead the index defined above

Table 2. Summary of Indexes and Indicators

Construct	% explained variance (KMO)	Indicators	% users answered "yes"
Suffered security attack on mobile	27.59 (0.56)	Malware mobile	1.57
		Not authorized use by someone	1.30
		Not authorized use by WiFi or Bluetooth	1.07
		Mobile Spam	22.88
		Wrong bill	5.46
		None of above	70.59
Mobile fraud	28.61 (0.66)	Received a phone call requesting user keys	1.17
		Received a message asking user keys	2.62
		Have received calls or messages with suspicious business deals to be fraudulent	8.92

		Have received on my mobile a request to open a file or a suspicious web link	6.91
		To use a service or app, have been asked to perform successive and excessive downloads or SMS	4.39
		Have discharged to services or mobile apps that had not signed	5.00
		None of above	79.52
Mobile security	39.40 (0.71)	Used any unlock mobile system (PIN, code…) after an inactivity period	59.20
		Had backups of contacts and/or another kind of data of your mobile	55.25
		Had free antivirus program in your mobile	32.86
		Had written down the serial number (IMEI) of the mobile terminal to lock in case of loss / theft	45.18
		Used tools to encrypt the information stored on the phone and / or protect communications by encrypting data leaving and entering the terminal	6.11
Mobile use	32.11 (0.75)	E-mail	78.42
		Geolocation services (Foursquare, Google Latitude, Facebook Places, Twitter Places, etc.)	34.87
		Access to free digital content (movies , music) or paid subscription (Spotify, Filmin , etc.)	35.14
		Social networks	69.94
		Games through mobile	46.94
		Electronic banking services	42.06
		E-commerce (shopping through mobile)	17.38

Note: Suffered security attack not include if the user lost the mobile or if the mobile has been stolen, although the survey included these items within this topic. KMO stands for Kaiser-Meyer-Olkin measure of sampling adequacy for performing PCA

Table 3. Frequency distribution of number of mobile attacks suffered in the last three months

# attacks	frequency	%	cum. %
0	1512	71.39	71.39
1	521	24.60	95.99
2	70	3.31	99.29
3	14	0.66	99.95
4	1	0.05	100.00
mean	0.3338	variance	0.3339
N=2118			

Table 4. Frequency distribution of number of mobile frauds suffered in the last three months

# frauds	frequency	%	cum. %
0	1,674	79.04	79.04
1	308	14.54	93.58
2	97	4.58	98.16
3	24	1.13	99.29
4	10	0.47	99.76
5 or more	5	0.24	100.00
mean	0.3021	variance	0.4792
N=2118			

3. Results

Table 5 presents the estimates of the different models (varying depending on the dependent variable definition and its way of measuring).

Table 5. Model estimates using Mobile security measures index.

Dependent variable	Mobile attack index	Number of Mobile attacks	Mobile attack (yes/no)	Mobile fraud index	#of Mobile frauds	Mobile fraud (yes/no)
Type of model	Linear regression	Poisson regression	Logit regression	Linear regression	Negative binomial regression	Logit regression
Mobile security measures index	**.064**** **(.027)**	**.070**** **(.030)**	**.124***** **(.045)**	**.087***** **(.028)**	**.117***** **(.041)**	**.101**** **(.040)**
Gender (1:male ;0:female)	.088 (.054)	.159** (.075)	.247** (.112)	.089 (.060)	.153 (.103)	.154 (.099)
Age	-.019 (.025)	.012 (.037)	-.010 (.055)	.016 (.030)	.050 (.050)	.009 (.049)
University degree (1:yes;0:no)	.141*** (.052)	.166** (.074)	.201* (.111)	.068 (.059)	.141 (.100)	.137 (.099)
Habitat size	.024 (.015)	.022 (.021)	.011 (.030)	-.001 (.016)	.014 (.027)	.031 (.027)
Mobile diversity use index	.045** (.019)	.150*** (.025)	.190*** (.039)	.114*** (.023)	.201*** (.035)	.181*** (.035)
Time being Internet user	-.766*** (.205)	-.584*** (.100)	-.838*** (.183)	-.577*** (.162)	-.562*** (.120)	-.762*** (.181)
Intensity of Internet use	-.408** (.193)	-.253* (.152)	-.795*** (.194)	-.412*** (.126)	-.494*** (.125)	-.123 (.215)
Constant	1.688*** (.640)	.0004 (.389)	-.014 (.636)	1.153** (.523)	-.524 (.438)	.859 (.638)
F (p-value)	4.88 (0.0000)			7.06 (0.0000)		
R^2	0.0464			0.0433		
Wald χ^2 (p-value)		99.80 (0.0000)	85.13 (0.0000)		87.38 (0.0000)	64.48 (0.0000)
Pseudo- R^2		0.0257	0.0375			0.0242
N	2118	2118	2118	2118	2118	2118

Notes: In parenthesis Robust Std. Error. * Significant at 10%, ** significant at 5% and *** significant at 1%.

Respect to the gender, it can be seen that there is some evidence that males are more likely suffer mobile security incidents, although there are not significant gender differences regarding frauds or fraud attempts. These results seem to support the general result that males are more likely to behave risky, and so they are more likely to have security pitfalls. However they finally react to these attacks and do not suffer more fraud incidents that women.

Regarding to the other demographics, age, education level and habitat it can be said that empirical results do not support the hypothesis raised in this paper. Neither the age nor the habitat size are significant variables in any of the models; therefore, hypothesis H1b is not empirically supported by the data. The case of the level of studies (measured by a dummy variable that takes value

one if the individual has a university degree and zero otherwise) is a bit more surprising, because it is significant and has a positive coefficient in all the models related to mobile attack. Therefore it has the opposite sign stated in hypothesis H1a. Results show that if a person has a university degree his or her level of mobile attack index is higher than if he or she does not have it, or is more likely to suffer an attack.

In relation to the variables that measure the level of knowledge about the Internet and mobile operating reached by means of experience, empirical results strongly support hypothesis H2a and H2b. Estimates show that the higher is the time being an Internet user and the higher is the intensity of use of Internet, the lower are the values both of mobile attack and mobile fraud indexes, and the lower are the probabilities of suffer any attack or fraud and, consequently, the number of attacks or frauds suffered. Thus, hypothesis H2a is strongly supported.

Besides that, the mobile diversity use index is positive and significant in all the models. Therefore, higher is the mobile diversity use index (i.e. the more different apps and mobile uses the individual does) the higher are the attack and fraud indexes, the likelihood of suffering an attack or fraud and the number of attacks or frauds suffered. Consequently, hypothesis H2b is also strongly supported.

Finally, the mobile security measures index has a positive and significant coefficient in all the models. The more protection and security measures an individual has implemented in his or her mobile device, the higher the values both of mobile attack and mobile fraud indexes, and the higher are the probabilities of suffer any attack or fraud and, consequently, the number of attacks or frauds suffered. Consequently it seems that data support hypothesis H3BIS instead of hypothesis H3. In other words, it seems to be some empirical support that the compensating risk theory is also operating in this field.

In order to check the robustness of this result, all the models have been estimated again by replacing this security measures index by a dummy variable that takes value one if the mobile user has an antivirus installed in his or her device and zero otherwise. Estimated results are shown in table 5bis. It can be seen that results remain almost equal, although levels of evidence in favour of H3bis are slightly lower (to have installed an antivirus is only one of the possible actions to be taken to be protected against cyber-attacks or frauds).

Table 5bis. Models estimates using mobile antivirus dummy instead mobile security measures index.

Dependent variable	Mobile attack index	Number of Mobile attacks	Mobile attack (yes/no)	Mobile fraud index	#of Mobile frauds	Mobile fraud (yes/no)
Type of model	Linear regression	Poisson regression	Logit regression	Linear regression	Negative binomial regression	Logit regression
Mobile antivirus	**.090***	**.139***	**.153**	**.126****	**.218****	**.110**
(1:yes; 0:no)	**(.046)**	**(.074)**	**(.096)**	**(.050)**	**(.010)**	**(.108)**
Gender	.096**	.162**	.153*	.128**	.225**	.261***
(1:male ;0:female)	(.046)	(.067)	(.088)	(.052)	(.094)	(.100)
Age	-.023	.010	.005	.011	.032	-.026
	(.0252	(.034)	(.044)	(.026)	(.045)	(.050)
University degree	.012	.002	.003	.002	.017	.018
(1:yes;0:no)	(.013)	(.019)	(.024)	(.014)	(.025)	(.027)
Habitat size	.120***	.171**	.170*	.097*	.203**	.245**
	(.045)	(.068)	(.090)	(.051)	(.092)	(.102)
Mobile diversity use	.052***	.158***	.193***	.128***	.233***	.217***
index	(.017)	(.022)	(.030)	(.021)	(.032)	(.035)
Time being Internet	-.588***	-.527***	-.640***	-.451***	-.493***	-.738***
user	(.164)	(0.96)	(.158)	(.131)	(.112)	(.160)
Intensity of Internet use	-.353**	-.272**	-.223	-.360***	-.486***	-.720***
	(.152)	(.125)	(.179)	(.107)	(.117)	(.173)
Constant	1.216**	-.219	.388	.701*	-.934**	-.345
	(.509)	(.353)	(.558)	(.419)	(.417)	(.563)
F	5.04			8.63		
(p-value)	(0.0000)			(0.0000)		
R^2	0.0330			0.0372		
Wald χ^2		97.45	68.21		96.35	92.14
(p-value)		(0.0000)	(0.0000)		(0.0000)	(0.0000)
Pseudo- R^2		0.0224	0.0209		0.0253	0.0336
N	2618	2618	2618	2618	2618	2618

Notes: In parenthesis Robust Std. Error. * Significant at 10%, ** significant at 5% and *** significant at 1%.

A criticism that can be made to this result is that it could be that the causality runs in the opposite way. That is, that the observed positive relationship (once other factors have been controlled) between level of security measures and level of attacks or frauds is due to that if an individual suffers an attack or a fraud, he or she will decide subsequently to increase his or her protection level. It could be the case, despite that the literality of the questions in the survey seems to indicate that the report of security incidents is restricted to the last three months whereas the questions related to the security measures installed seem to be referred to a wider time span.

4. Conclusion

With this paper, it is shown that variables like age and gender are very significatively to explain the attacks. Almost the education and known that there is a security problem using mobile affects positively on the probability to don’t have a mobile attack.

A surprising result is that having lots of protection tools can cause "false confidence" feelings, and therefore, make you behave with more risk, conversely to what was supposed.

One limitation of this study is that the survey doesn’t have a question about if the individual starts to use security mobile after or before an attack. This question is important to have for know better the situation.

A policy recommendation is that the government should educate to people at school, high school, university and also at work, because if people know that there is a security problem using the mobile, they could take care and try to protect themselves.

REFERENCES

Butler, M. J. (2014). Towards online security: key drivers of poor user behaviour and recommendations for appropriate interventions. *South African Journal of Business Management,* 45(4), 21-32.

Byrnes, J. P., Miller, D. C., & Schafer, W. D. (1999). Gender differences in risk taking: A meta-analysis. *Psychological bulletin*, *125*(3), 367.

Christin, N., Egelman, S., Vidas, T., & Grossklags, J. (2011, February). It's all about the Benjamins: An empirical study on incentivizing users to ignore security advice. In *International Conference on Financial Cryptography and Data Security* (pp. 16-30). Springer Berlin Heidelberg.

Jin, L., Chen, Y., Wang, T., Hui, P., & Vasilakos, A. V. (2013). Understanding user behaviour in online social networks: A survey. *Communications Magazine, IEEE,* 51(9), 144-150.

Paulsen, D. J., Platt, M. L., Huettel, S. A., & Brannon, E. M. (2012). From risk-seeking to risk-averse: the development of economic risk preference from childhood to adulthood. *Frontiers in psychology*, *3*, 313.

Pearman, S., Kumar, A., Munson, N., Sharma, C., Slyper, L., Bauer, L., and Christin, N. (2016) Risk Compensation in Home-User Computer Security Behaviour: A Mixed-Methods Exploratory Study. *Poster presented at SOUPS 2016 (Twelfth Symposium on Usable Privacy and Security)*

Telefónica, F. (2016). *La sociedad de la información en España 2015*. Fundación Telefónica.

Wilde, G.J.S. (1998). Risk Homeostasis Theory: An Overview. *Injury Prevention* 4, 89–91.