information

MDPI

Article

Virtual Offenses: Role of Demographic Factors and Personality Traits †

Frantisek Sudzina [1,2] and Antonin Pavlicek [2,*]

[1] Department of Business and Management, Faculty of Social Sciences, Aalborg University, 9220 Aalborg, Denmark; sudzina@business.aau.dk
[2] Faculty of Informatics and Statistics, University of Economics, 130 67 Prague, Czech Republic
* Correspondence: antonin.pavlicek@vse.cz; Tel.: +420-224-095-473
† This is an extended version of our conference paper presented in the Interdisciplinary Information Management Talks (IDIMT 2018), Kutná Hora, Czech Republic, 6 September 2018.

Received: 31 January 2020; Accepted: 29 March 2020; Published: 31 March 2020

Abstract: A number of positive and negative trends are becoming more prevalent, along with the widespread use of information and communication technologies in everyday life—negative ones being virtual offences such as stalking, bullying, identity theft, scamming and abuse or harassment. The article discusses the relations between demographic factors, the occurrence of virtual offenses and personality traits. The next Big Five Inventory (BFI-2) was used for assessment of personality traits. As for the findings, more extraversion, less agreeableness, more negative emotionality, less consciousness and being a man have been found to be associated with at least one of the investigated types of virtual offenses.

Keywords: virtual offenses; demographic factors; personality traits

1. Introduction

Together with the invention and the expansion of electronics, computers and computer networks in everyday life, criminal activities are also moving into this area. In addition to traditional crimes that existed in the offline environment, we have also witnessed a whole new criminal acts that arose as a result of these new technologies. We talk about cybercrime and virtual offences.

Cybercrime or computer-oriented crime is commonly defined as a malicious activity that uses a computer and/or a computer network either in the commission of a crime, or as the target. It includes the usage of internet (social networks, emails or chat software) and even mobile phones.

Cybercrime may threaten victim's personality, privacy, security and often financial interests. Issues surrounding cybercrime may include: unwarranted surveillance and data gathering, identity theft, harassment, bullying, sextortion, stalking, child pornography, hacking. These harmful acts committed on-line are usually already prohibited by the existing criminal law. Harassment, threatening violence, stalking, malicious communications, incitement and theft are all crimes from off-line era. Cyberspace makes them easier to commit and harder to stop and punish—that is why cybercrimes are becoming widespread lately. It does not mean that we resign and accept them as a new norm. Common law defines criminal offences as acts (or omissions) which are so harmful that the wrong is thought to be against the state rather than the individual who has suffered the act; the state prosecutes and, on conviction by a court, the state punishes, by deprivation of liberty, fine or other means [1].

While cybercrime involves serious crimes such as financial fraud, cyberterrorism and cyberextortion is not the subject of our research, this paper focuses on less serious forms of crime—virtual offenses.

Virtual offences which we focus on are:

- identity theft—unauthorized use of someone else's identity to gain benefits in the other person's name. Based on theft of personally identifying information and its subsequent use for criminal activities. The victim is left with consequences (invoices, charges and a damaged personal credit).
- cyber stalking (e-stalking or online stalking)—use of electronic means to systematically stalk, embarrass or threaten a victim. It may also include defamation, false accusations, or libel. Cyber stalking is perpetrated through social media, email, instant messaging as well as other electronic media.
- phishing—fraudulent act of acquiring sensitive private information such as account passwords, personal identification details, usernames, credit card info, social security numbers by using a complex set of social engineering techniques and pretending to be a trustworthy entity in an electronic communication.
- cyber scam—a form of fraud (confidence tricks) promising the victim a significant financial benefit conditioned by a minor up-front payment. The Federal Bureau of Investigation (FBI) defines cyber scam as an advance fee scheme in which the victim pays money to someone in anticipation of receiving something of greater value—such as a loan, contract, investment, or gift—and then receives little or nothing in return. Notoriously popular became so called Nigerian scams offering a share in a large sum of money or a payment for help to transfer money out of the country.
- cyber harassment—harassment conducted by the social media, email, instant messaging or other electronic means. It can be in the form of unwanted sexually explicit messages, pictures (so called dickpics), inappropriate or offensive advances, threats of physical and/or sexual violence and/or hate speech (insults, threats).

A quite interesting topic—related to the virtual offences and cybercrime—is theft limited to the digital environment. W. Rumbles in his article in Canterbury Law Review asks interesting question: Theft in the digital: Can you steal virtual property? [2]. Rumbles introduces a number of counter intuitive concepts related to the extending real world criminal liability and criminal law to behavior and activities inside purely virtual worlds (Second Life, on-line game environments like World of Warcraft). He looks into the theft of virtual property and explores how different jurisdictions are responding to the evolution of virtual property.

Virtual offences are unfortunately becoming quite common. Very illustrative case is so called GamerGate controversy, which refers to a 2014 harassment campaign conducted primarily through the use of the #GamerGate hashtag. It opens issues of sexism and progressivism in video game culture, which attracted public attention, but other cases of online offences are usually underreported. However, academic literature does cover some cases of virtual offences. For example Bailey Poland [3] covers the latest available research into cybersexism and questions its motivations, monitors related activities and explores different methods of Internet misogyny reduction.

Yi-Chih Lee and Wei-Li Wu in their 2018 article Factors in cyber bullying: the attitude-social influence-efficacy model [4] examine the correlation between social influence, knowledge, self-efficacy, risk perception and cyberbullying behavior from the perspective of the attitude-social influence-efficacy model—particularly for youngsters who have an admitted history of cyberbullying behavior or have observed their peers' cyberbullying behavior. Yi-Chih Lee et al. conclude that attitude towards cyberbullying affected cyberbullying intention, and vice versa that intention influenced witnessed cyberbullying behavior.

Justin W. Patchin [5] surveyed a sample of almost 5 thousand US middle and high school students (age 12–17) and realized that 36.5% reported experiencing cyberbullying in their lifetimes; 17.4% in the previous 30 days. Reported problems include: Mean or hurtful online comments, rumors spread, threats to hurt through a cell phone text, mean names or comments with sexual meaning, impersonation, mean or hurtful picture or video, insults to race, color, religion, mean or hurtful web page, cyberbullying by gender. As for the gender of victims, adolescent girls are slightly more likely to have experienced cyberbullying than boys (38.7% to 34.1%), boys on the other hand were more likely to

confess to be perpetrators (16.1% to 13.4%). The 2019 findings are quite consistent with similar surveys in 2010, 2015 and 2016, which proves that the problem of cyberbullying is a persistent problem.

However, online cruelty is not limited just to adolescents, adults get cyberbullied too. In this case the perpetrators, commonly referred to as trolls, are basking in anonymity which gives them possibility to abuse and harass a victim without fear of consequences. Famous personalities, such as actors, politicians, musicians, athletes and other VIPs get cyberbullied routinely and report the distress it causes to them [6].

Aiken, M. [7] in the book The Cyber Effect describes the psychological phenomenon of Diffusion of Responsibility in relation to cyberbullying or harassment. Diffusion of Responsibility implies the greater the number of people who witness a crime or emergency, the less likely any of them will feel responsible to respond. It is also sometimes called The Bystander Effect and, in case of cyberbullying, hundreds to thousands of people can witness bullying online on a regular basis but do not step up and do anything about it.

To prevent cyberbullying social media can employ advanced social analytics not just to estimate user's age, sex and political leanings, but also use mathematical algorithms to detect antisocial behavior, bullying or harassment. By analyzing behavioral parameters, content analysis (usage of keywords such as die, hate, bastard, etc.) can estimate the direction, length and frequency of attacks.

As for the literature where online offences have already been linked to the personality traits, there is not much so far. So far the best research in this area has been done by Steve G. A. van de Weijer and E. Rutger Leukfeldt in their article [8] Big Five Personality Traits of Cybercrime Victims published in Cyberpsychology, Behavior and Social Networking.

Their study based on a large (N = 3648) representative sample of Dutch population focused on the link between the victimization of cybercrime and the main characteristics of the Big Five personality model, which is exactly what authors have done in this paper. De Weijer et al. used multinomial logistic regression analyzes to explore correlations between the specific personality characteristics and 3 classes of victims (victims of cybercrime against non-victims, victims of traditional crime against non-victims and victims of cybercrime against victims of conventional crime). As opposed to our research, de Weijer et al. [8] divided crimes into two separated groups—cyber-dependent crimes (i.e., computer virus spreading and cracking) and cyber-enabled crimes (i.e., virtual coercion, bank account robbery and consumer fraud) and used logistic regression to predict victimization, stating that there is only a minor difference between identified Big Five personality traits related to the victimization of both cyber-dependent and/or cyber-enabled misconducts.

Interesting finding is, that Big Five personality characteristics are not directly correlated with victimization in cyberspace but rather with the victimization in general (both off-line and on-line). Only those with higher emotional health ratings were less likely to fall victim to criminal in the cyber space than conventional crime in the real world. Only respondents more opened to experience would have greater chances of becoming cyber-enabled crime victim.

Thomas J. Holt et al. [9] in his article Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization studied the connection between low self-control and increased risk of victimization. He theorized that the increase is due to frequent involvement in routine activities that tend to place victims into the close proximity of motivated perpetrators (e.g., downloading files, visiting questionable websites) and decrease in their willingness to use adequate preventive steps (antivirus and wireless network protection). This link is significant not only in predicting physical forms of victimization, but also crime in the cyberspace.

Importance of self-control and utilizing of appropriate guardianship factor are studied also in the article [10] Privacy-Preserving Content-Oriented Wireless Communication in Internet-of-Things. Author points out that with the growing number of GSM and Internet-linked devices (e.g., simple sensors), the capacity to ensure security without incurring unrealistic performance overheads is crucial. Instead of using conventional encryption authors suggest the dynamic privacy protection model designed to achieve improved privacy protection even in large volume of data transmissions.

The authors also developed the approach called a fully homomorphic encryption (FHE) for blend operations model that uses tensor laws to carry the computations of blend arithmetic operations over real numbers [11].

Personality Traits

Hinds, Tung, Franz et al. in the article Genome-wide Analyses for Personality Traits Dentify Six Genomic Loci and Show Correlations with Psychiatric Disorders [12] conclude that Big Five personality traits are genetically dependent. The meta-analysis Patterns of mean-level change in personality traits across the life course: a meta-analysis of longitudinal studies [13] points out that people are more conscientious, more agreeable and emotionally positive as they grow older. Another meta-analysis worth mentioning is A Systematic Review of Personality Trait Change Through Intervention [14], which concludes that negative emotionality and extraversion can be possibly cured by therapy. When we take into consideration quite young age of our respondents, they could have been victims of a virtual offense only recently, there is not enough time for the effect of aging (identified by [13]).

The gender aspect in the field of information and communication technologies has been studied in extensively [15], however we have not found any study related to the virtual offenses. The problematics of virtual offenses and personality traits is quite comprehensive and is influenced (amongst others) by ethics [16], psychology [17] and education theory [18].

The main goal of our investigation is to establish if demographic factor or Big Five personality traits may be connected to online offenses.

Unfortunately, since we are using a cross-sectional survey, it does not allow us to test also causality, in other words, whether Big Five personality traits caused the respondent to be a victim of a virtual crime or the experience of virtual crime changed Big Five personality traits of the subject.

The article is structured in the traditional format: the next section Methodology describes data collection and method of analysis. In the section Results, the overall tables of the analysis are presented. The section Discussion tries to explain our findings in relation to similar works and known facts. The last section offers brief conclusions.

2. Methodology

2.1. Data

The research was conducted in December 2017–March 2018. Data were collected using a web-based questionnaire. The sample consisted of 478 university students (206 women, 272 men; average age 20.5 years) from the Czech Republic. With regards to their work experience, 12 hold a full-time position within the field of study, 16 hold a full-time positon outside the field of study, 164 are employed part-time, 176 are in temporary employment and 106 do not work at all, just study.

Personality of respondents was assessed using Big Five Inventory 2 from John and Soto [19], more specifically, using a standard Czech translation by Hřebíčková et al. [20] (this time we have not used the short 15-statement version, BFI-2-XS [21], which was employed in the conference paper [22] from which this article is derived).

There will be five models because the article studies five virtual offenses. The dependent variables for these five models were assessed using the question Have you encountered any other form of virtual offense? Possible answers for each virtual offence (identity theft, stalking, phishing, scam and harassment) were:

- No (coded as 0),
- Yes, but I managed to defend myself (coded as 1),
- Yes, and I was a victim (coded as 2).

The survey included also other questions but they were not used in this article.

2.2. Method

Since the dependent variables—virtual offences—were measured on the ordinal scale (where it is not possible to assume that there is the same distance between "no" and "yes, but I managed to defend myself" and between "yes, but I managed to defend myself" and "yes, and I was a victim"), ordinal logistic regression [23] will be used. The independent variables are demographics (gender, age, work alongside studies) and personality (five traits). We employ a multi-variate approach, i.e., test the impact of all independent variables in one step, as opposed to a bi-variate approach which would test impact of only one independent variable on the dependent variable in one step. For each virtual offence, two models will be provided. Oddly numbered tables will provide regression models with all independent variables, and evenly numbered tables will provide streamlined regression models which contain only independent variables that significantly influence the dependent variable. Removal of insignificant independent variables tends to improve significance of the remaining variables. Pseudo-R2s will be used to describe the explanatory power of each model. The calculations were conducted in IBM SPSS 22.

3. Results

Model 1 estimates influence of demographics and personality on identity theft. Regression coefficients are shown in Table 1. With regards to the explanatory power, Cox and Snell pseudo-R2 is 0.030, Nagelkerke pseudo-R2 is 0.041, McFadden pseudo-R2 is 0.024 and *p*-value is 0.215.

Table 1. Full Model 1—Identity theft: ordinal logistic regression.

Variable	B	S.E.	Wald	df	Sig.
Identity theft = 0	−0.126	1.846	0.005	1	0.946
Identity theft = 1	1.203	1.849	0.424	1	0.515
Extraversion	0.299	0.199	2.261	1	0.133
Agreeableness	−0.446	0.216	4.254	1	0.039
Conscientiousness	0.116	0.189	0.372	1	0.542
Negative emotionality	−0.049	0.178	0.075	1	0.785
Openness to experience	−0.022	0.207	0.011	1	0.917
Age	−0.033	0.051	0.437	1	0.509
Part-time job	−0.258	0.662	0.152	1	0.696
Studies only	−0.315	0.687	0.211	1	0.646
Temporary job	−0.645	0.671	0.922	1	0.337
Full-time job outside the field of studies	0.041	0.836	0.002	1	0.961
Full-time job within the field of studies	0 [a]	.	.	0	.
Male	−0.005	0.251	0.000	1	0.984
Female	0 [a]	.	.	0	.

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; df = Degrees of Freedom; Wald = Wald Test; Sig = Significance. [a] Parameter is redundant (male OR female, outside OR inside).

Regression coefficients for the streamlined model for identity theft are shown in Table 2. With regards to the explanatory power, Cox and Snell pseudo-R2 is 0.022, Nagelkerke pseudo-R2 is 0.030, McFadden pseudo-R2 is 0.017 and *p*-value is 0.005.

Model 2 estimates influence of demographics and personality on stalking. Regression coefficients are shown in Table 3. With regards to the explanatory power, Cox and Snell pseudo-R2 is 0.062, Nagelkerke pseudo-R2 is 0.088, McFadden pseudo-R2 is 0.053 and *p*-value is 0.001.

Table 2. Streamlined Model 1—Identity theft: ordinal logistic regression.

Variable	B	S.E.	Wald	df	Sig.
Identity theft = 0	0.860	0.881	0.954	1	0.329
Identity theft = 1	2.179	0.891	5.978	1	0.014
Extraversion	0.369	0.167	4.892	1	0.027
Agreeableness	−0.491	0.201	5.942	1	0.015

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; df = Degrees of Freedom; Wald = Wald Test; Sig = Significance.

Table 3. Full Model 2—Stalking: ordinal logistic regression.

Variable	B	S.E.	Wald	df	Sig.
Stalking = 0	−3.057	1.919	2.538	1	0.111
Stalking = 1	−1.630	1.915	0.724	1	0.395
Extraversion	0.454	0.208	4.756	1	0.029
Agreeableness	−0.782	0.230	11.578	1	0.001
Conscientiousness	−0.046	0.199	0.054	1	0.816
Negative emotionality	0.084	0.186	0.202	1	0.653
Openness to experience	−0.298	0.216	1.895	1	0.169
Age	−0.013	0.054	0.054	1	0.816
Part-time job	−1.879	0.597	9.901	1	0.002
Studies only	−1.927	0.632	9.301	1	0.002
Temporary job	−1.925	0.602	10.232	1	0.001
Full-time job outside the field of studies	−2.116	0.876	5.838	1	0.016
Full-time job within the field of studies	0 [a]	.	.	0	.
Male	−0.379	0.262	2.087	1	0.149
Female	0 [a]	.	.	0	.

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; Wald = Wald Test; df = Degree of Freedom; Sig = Significant. [a] This parameter is set to zero because it is redundant (male OR female, outside OR inside).

Regression coefficients for the streamlined model for stalking are shown in Table 4. With regards to the explanatory power, Cox and Snell pseudo-R2 is 0.058, Nagelkerke pseudo-R2 is 0.083, McFadden pseudo-R2 is 0.050 and *p*-value is 0.000.

Table 4. Streamlined Model 2—Stalking: ordinal logistic regression.

Variable	B	S.E.	Wald	df	Sig.
Stalking = 0	−2.433	1.188	4.198	1	0.040
Stalking = 1	−1.000	1.185	0.711	1	0.399
Extraversion	0.338	0.182	3.454	1	0.063
Agreeableness	−0.833	0.222	14.087	1	0.000
Part-time job	−1.885	0.590	10.208	1	0.001
Studies only	−1.938	0.627	9.568	1	0.002
Temporary job	−1.886	0.593	10.096	1	0.001
Full-time job outside the field of studies	−2.196	0.865	6.449	1	0.011
Full-time job within the field of studies	0 [a]	.	.	0	.
Male	−0.428	0.246	3.041	1	0.081
Female	0 [a]	.	.	0	.

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; df = Degrees of Freedom; Wald = Wald Test; Sig = Significance. [a] Parameter is redundant (male OR female, outside OR inside).

If extraversion and genders are excluded, significance of the regression coefficient for the threshold of 0 improves to 0.001 and for the threshold of 1 it changes to 0.081. With regards to the explanatory power, Cox and Snell pseudo-R2 changes to 0.045, Nagelkerke pseudo-R2 to 0.064, McFadden pseudo-R2 to 0.038 and *p*-value to 0.001.

Model 3 estimates influence of demographics and personality on phishing. Regression coefficients are shown in Table 5. With regards to the explanatory power, Cox and Snell pseudo-R2 is 0.061, Nagelkerke pseudo-R2 is 0.080, McFadden pseudo-R2 is 0.044 and *p*-value is 0.002.

Table 5. Full Model 3—Phishing: ordinal logistic regression.

Variable	B	S.E.	Wald	df	Sig.
Phishing = 0	0.063	1.736	0.001	1	0.971
Phishing = 1	2.055	1.742	1.391	1	0.238
Extraversion	0.135	0.181	0.556	1	0.456
Agreeableness	−0.233	0.198	1.388	1	0.239
Conscientiousness	−0.252	0.175	2.067	1	0.151
Negative emotionality	0.098	0.161	0.371	1	0.542
Openness to experience	−0.025	0.190	0.018	1	0.894
Age	0.031	0.050	0.383	1	0.536
Part-time job	−0.866	0.590	2.156	1	0.142
Studies only	−0.876	0.616	2.018	1	0.155
Temporary job	−1.425	0.603	5.590	1	0.018
Full-time job outside the field of studies	−0.677	0.762	0.790	1	0.374
Full-time job within the field of studies	0 [a]	.	.	0	.
Male	0.737	0.240	9.421	1	0.002
Female	0 [a]	.	.	0	.

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; df = Degrees of Freedom; Wald = Wald Test; Sig = Significance. [a] Parameter is redundant (male OR female, outside OR inside).

Regression coefficients for the streamlined model for phishing are shown in Table 6. With regards to the explanatory power, Cox and Snell pseudo-R2 is 0.050, Nagelkerke pseudo-R2 is 0.066, McFadden pseudo-R2 is 0.036 and *p*-value is 0.000.

Table 6. Streamlined Model 3—Identity theft: ordinal logistic regression.

Variable	B	S.E.	Wald	df	Sig.
Phishing = 0	0.581	0.584	0.989	1	0.320
Phishing = 1	2.570	0.606	18.008	1	0.000
Part-time job	−0.737	0.583	1.602	1	0.206
Studies only	−0.835	0.597	1.952	1	0.162
Temporary job	−1.326	0.589	5.065	1	0.024
Full-time job outside the field of studies	−0.438	0.748	0.343	1	0.558
Full-time job within the field of studies	0 [a]	.	.	0	.
Male	0.809	0.225	12.979	1	0.000
Female	0 [a]	.	.	0	.

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; df = Degrees of Freedom; Wald = Wald Test; Sig = Significance. [a] Parameter is redundant (male OR female, outside OR inside).

Model 4 estimates influence of demographics and personality on scam. Regression coefficients are shown in Table 7. With regards to the explanatory power, Cox and Snell pseudo-R2 is 0.117, Nagelkerke pseudo-R2 is 0.141, McFadden pseudo-R2 is 0.071 and *p*-value is 0.000.

Regression coefficients for the streamlined model for scam are shown in Table 8. It is worth noting that the reference category was changed from the full-time job within the field of study to the full-time job outside the field of study. With regards to the explanatory power, Cox and Snell pseudo-R2 is 0.111, Nagelkerke pseudo-R2 is 0.134, McFadden pseudo-R2 is 0.067 and *p*-value is 0.000.

Table 7. Full Model 4—Scam: ordinal logistic regression.

Variable	B	S.E.	Wald	df	Sig.
Scam = 0	0.336	1.597	0.044	1	0.833
Scam = 1	2.473	1.603	2.380	1	0.123
Extraversion	−0.102	0.165	0.382	1	0.537
Agreeableness	0.053	0.181	0.087	1	0.769
Conscientiousness	−0.415	0.159	6.785	1	0.009
Negative emotionality	0.188	0.146	1.657	1	0.198
Openness to experience	0.223	0.173	1.659	1	0.198
Age	0.008	0.045	0.028	1	0.867
Part-time job	−0.788	0.584	1.820	1	0.177
Studies only	−0.718	0.604	1.411	1	0.235
Temporary job	−1.035	0.589	3.087	1	0.079
Full-time job outside the field of studies	−0.072	0.741	0.009	1	0.923
Full-time job within the field of studies	0 [a]	.	.	0	.
Male	1.221	0.219	31.093	1	0.000
Female	0 [a]	.	.	0	.

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; df = Degree of Freedom; Wald = Wald Test; Sig = Significant. [a] Parameter is redundant (male OR female, outside OR inside).

Table 8. Streamlined Model 4—Scam: ordinal logistic regression.

Variable	B	S.E.	Wald	df	Sig.
Scam = 0	−1.144	0.722	2.510	1	0.113
Scam = 1	0.997	0.722	1.904	1	0.168
Conscientiousness	−0.441	0.153	8.343	1	0.004
Part-time job	−0.809	0.507	2.549	1	0.110
Studies only	−0.715	0.519	1.894	1	0.169
Temporary job	−1.047	0.508	4.251	1	0.039
Full-time job outside the field of studies	0 [a]	.	.	0	
Full-time job within the field of studies	−0.023	0.733	0.001	1	0.975
Male	1.160	0.205	32.110	1	0.000
Female	0 [a]	.	.	0	.

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; df = Degrees of Freedom; Wald = Wald Test; Sig = Significance. [a] Parameter is redundant (male OR female, outside OR inside).

Model 5 estimates influence of demographics and personality on harassment. Regression coefficients are shown in Table 9. With regards to the explanatory power, Cox and Snell pseudo-R2 is 0.041, Nagelkerke pseudo-R2 is 0.053, McFadden pseudo-R2 is 0.029 and *p*-value is 0.047.

Regression coefficients for the streamlined model for harassment are shown in Table 10. It is worth noting that the reference category was changed from the full-time job within the field of study to the full-time job outside the field of study. With regards to the explanatory power, Cox and Snell pseudo-R^2 is 0.035, Nagelkerke pseudo-R^2 is 0.046, McFadden pseudo-R^2 is 0.024 and *p*-value is 0.009.

If gender is excluded in the streamlined model, significance of the regression coefficient for the threshold of 0 improves to 0.046 and for the threshold of 1 it changes to 0.000. With regards to the explanatory power, Cox and Snell pseudo-R2 changes to 0.028, Nagelkerke pseudo-R2 to 0.037, McFadden pseudo-R2 to 0.020 and *p*-value to 0.017.

Table 9. Full Model 9—Harassment: ordinal logistic regression.

Variable	B	S.E.	Wald	Df	Sig.
Harassment = 0	−0.247	1.750	0.020	1	0.888
Harassment = 1	1.092	1.752	0.388	1	0.533
Extraversion	0.138	0.183	0.571	1	0.450
Agreeableness	−0.270	0.205	1.741	1	0.187
Conscientiousness	0.034	0.173	0.039	1	0.843
Negative emotionality	0.321	0.163	3.886	1	0.049
Openness to experience	−0.114	0.191	0.356	1	0.551
Age	−0.021	0.050	0.184	1	0.668
Part-time job	−0.815	0.615	1.760	1	0.185
Studies only	−1.065	0.642	2.748	1	0.097
Temporary job	−0.754	0.615	1.502	1	0.220
Full-time job outside the field of studies	0.154	0.765	0.041	1	0.840
Full-time job within the field of studies	0 [a]	.	.	0	.
Male	−0.425	0.230	3.402	1	0.065
Female	0 [a]	.	.	0	.

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; df = Degrees of Freedom; Wald = Wald Test; Sig = Significance. [a] Parameter is redundant (male OR female, outside OR inside).

Table 10. Streamlined Model 5—Harassment: ordinal logistic regression.

Variable	B	S.E.	Wald	df	Sig.
Harassment = 0	0.788	0.710	1.233	1	0.267
Harassment = 1	2.120	0.719	8.700	1	0.003
Negative emotionality	0.331	0.150	4.871	1	0.027
Part-time job	−1.040	0.518	4.021	1	0.045
Studies only	−1.317	0.542	5.915	1	0.015
Temporary job	−1.047	0.516	4.122	1	0.042
Full-time job outside the field of studies	0 [a]	.	.	0	.
Full-time job within the field of studies	−0.160	0.748	0.046	1	0.831
Male	−0.396	0.220	3.246	1	0.072
Female					

Key: B = Regression Coefficient Beta; S.E. = Standard Error of B; df = Degrees of Freedom; Wald = Wald Test; Sig = Significance. [a] Parameter is redundant (male OR female, outside OR inside).

4. Discussion

We have tested 5 different models in our paper. Model 1 estimates influence of demographics and personality on identity theft, model 2 estimates influence of demographics and personality on stalking, model 3 estimates influence of demographics and personality on phishing, model 4 estimates influence of demographics and personality on scam and model 5 estimates influence of demographics and personality on harassment. Here are our most important findings.

(1). More extravert individuals are more prone to become the victims of identity theft. This finding is not so surprising and confirms the assumption that identity theft usually requires an access to the victims and extraversion tends to cause that—people high in extraversion enjoy engaging with the external world, often seek out the company of other people. They are action-oriented and enthusiastic, people, who tend to thrive on excitement, they are quite open and it increases the chances they put themselves into the positions leading to the identity theft.

(2). As for stalking, less agreeable individuals are more prone to be victims of stalking. An explanation could be, that people who score low on the scale of agreeableness usually put their own interests above interests of others. They are inclined to be uncooperative, unfriendly and distant, and therefore stalkers can be incentivized to use them for target practice.

(3). Another reasonable result is that more neurotic individuals are prone to report being harassment victims. A person who scores high in neuroticism is emotionally very reactive, he/she

feels vulnerable or in a bad mood even in quite standard situation. He/she has an emotional reaction to events and activities that would probably not affect other people. They may find it difficult to cope with stress and think clearly. So reported victimization can be explained by oversensitivity and self-victimization.

(4). Less consciousness individuals are more prone to be victims of scam. Since conscientiousness is ability to regulate, control and direct urges and impulses, the less control a person have over his impulses, the more prone he is to be scammed.

(5). We also came to some findings, which are not easily explain. It seems, that men report to be more often a victim of scam and phishing. Why that is should be researched later, we do not have any theory for that at the moment. In addition, respondents who work full-time outside their field of studies report to be victims of scam and harassment, while full-time workers within their field of studies suffer from stalking and phishing. Last but not least, less agreeable people seem to be more often victims of identity theft. These findings will have to be subject of further investigation.

When we compare our findings with van de Weijer's article [8] Big Five Personality Traits of Cybercrime Victims, we can confirm their observations and conclusions. They have found that people with higher emotional stability were less likely to be a victim of cybercrime which was confirmed by our statistics, since our results indicate that people with lower scores (neurotics) are more prone to report being victims of harassment. As for their conclusion that people opened to experience have higher chances to become a victim of cyber-enabled crimes, we have found that other similar factor (extraversion) can play a role. Again, not surprising, since openness and extraversion are correlated [24].

5. Conclusions

The paper tried to answer the question, whether individuals with certain demographics and personality traits are more likely to become victims of virtual offenses. Five different kinds of virtual offenses were researched—stalking, identity theft, harassment, scam and phishing. It shows, that less agreeable and more extravert individuals are more prone to become the victims of identity theft. As for stalking, full-time workers within their field of studies and less agreeable individuals are more prone to be victims of stalking. More neurotic individuals and respondents who work full time outside their field of studies are more prone to be victims of harassment. Less consciousness individuals, respondents who work full time outside their field of studies and men are more prone to be victims of scam. Respondents who work full time within their field of studies and men are more prone to be victims of phishing. If taking only personality traits significant at 0.05 level into consideration, it is more likely to become a victim of a virtual offense if one is more extravert, more neurotic, less agreeable, less consciousness and a male.

Author Contributions: Conceptualization, F.S. and A.P.; methodology, F.S.; validation A.P.; formal analysis, F.S.; investigation, A.P.; resources A.P.; data curation, A.P.; writing—original draft preparation, A.P., F.S.; writing—review and editing, A.P.; project administration, F.S.; funding acquisition, A.P. All authors have read and agreed to the published version of the manuscript.

Funding: Paper was processed with contribution from the University of Economics in Prague, IG Agency, grant number F4/27/2019.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. House of Lords—Social Media and Criminal Offences—Communications Committee. Available online: https://publications.parliament.uk/pa/ld201415/ldselect/ldcomuni/37/3704.htm (accessed on 14 January 2019).
2. Rumbles, W. Theft in the digital: Can you steal virtual property? *Canterb. Law Rev.* **2011**, *17*, 354–374.
3. Poland, B. *Haters: Harassment, Abuse, and Violence Online*; Potomac Books: Lincoln, NE, USA, 2016; ISBN 978-1-61234-766-0.

4. Lee, Y.-C.; Wu, W.-L. Factors in cyber bullying: The attitude-social influence-efficacy model. *An. Psicol.* **2018**, *34*, 324–331. [CrossRef]
5. Cyberbullying Research Center 2016 Cyberbullying Data. Available online: https://cyberbullying.org/2016-cyberbullying-data (accessed on 5 January 2018).
6. Rao, T.S.S.; Bansal, D.; Chandran, S. Cyberbullying: A virtual offense with real consequences. *Indian J. Psychiatry* **2018**, *60*, 3–5.
7. Aiken, M. *The Cyber Effect: An Expert in Cyberpsychology Explains How Technology Is Shaping Our Children, Our Behavior, and Our Values—And What We Can Do About It*; Reprint ed.; Spiegel & Grau: New York, NY, USA, 2017; ISBN 978-0-8129-8747-8.
8. Van de Weijer, S.G.A.; Leukfeldt, E.R. Big Five Personality Traits of Cybercrime Victims. *Cyberpsychol. Behav. Soc. Netw.* **2017**, *20*, 407–412. [CrossRef] [PubMed]
9. Holt, T.J.; Wilsem, J.; van Weijer, S. van de Leukfeldt, R. Testing an Integrated Self-Control and Routine Activities Framework to Examine Malware Infection Victimization. *Soc. Sci. Comput. Rev.* **2018**, *38*, 187–206. [CrossRef]
10. Gai, K.; Choo, K.-K.R.; Qiu, M.; Zhu, L. Privacy-Preserving Content-Oriented Wireless Communication in Internet-of-Things. *IEEE Internet Things J.* **2018**, *5*, 3059–3067. [CrossRef]
11. Gai, K.; Qiu, M. Blend Arithmetic Operations on Tensor-Based Fully Homomorphic Encryption Over Real Numbers. *IEEE Trans. Ind. Inform.* **2018**, *14*, 3590–3598. [CrossRef]
12. Lo, M.-T.; Hinds, D.A.; Tung, J.Y.; Franz, C.; Fan, C.-C.; Wang, Y.; Smeland, O.B.; Schork, A.; Holland, D.; Kauppi, K.; et al. Genome-wide analyses for personality traits identify six genomic loci and show correlations with psychiatric disorders. *Nat. Genet.* **2017**, *49*, 152–156. [CrossRef] [PubMed]
13. Roberts, B.W.; Walton, K.E.; Viechtbauer, W. Patterns of mean-level change in personality traits across the life course: A meta-analysis of longitudinal studies. *Psychol. Bull.* **2006**, *132*, 1–25. [CrossRef] [PubMed]
14. Roberts, B.W.; Luo, J.; Briley, D.A.; Chow, P.I.; Su, R.; Hill, P.L. A systematic review of personality trait change through intervention. *Psychol. Bull.* **2017**, *143*, 117–141. [CrossRef] [PubMed]
15. Nedomová, L.; Maryska, M.; Doucek, P. Unequal wage of men and women in ICT in the Czech Republic? *Gender, Technol. Dev.* **2017**, *21*, 116–134. [CrossRef]
16. Sigmund, T. Ethics in the Cyberspace. IDIMT-2013: Information Technology Human Values, Innovation and Economy. *SJR* **2013**, *42*, 269–279.
17. Potancok, M.; Vondrova, D.; Andera, M. *Psychological Aspects and Barriers of Ehealth Implementation*; Petr, D., Gerhard, C., Vaclav, O., Eds.; Universitatsverlag Rudolf Trauner: Linz, Austria, 2015; Volume 44, ISBN 978-3-99033-395-2.
18. Vondra, Z. *Initiative to Support Use of Social Media Functions to Improve Education Effect*; Petr, D., Gerhard, C., Vaclav, O., Eds.; Trauner Verlag: Linz, Austria, 2017; Volume 46, ISBN 978-3-99062-119-6.
19. Soto, C.J.; John, O.P. The next Big Five Inventory (BFI-2): Developing and assessing a hierarchical model with 15 facets to enhance bandwidth, fidelity, and predictive power. *J. Pers. Soc. Psychol.* **2017**, *113*, 117–143. [CrossRef] [PubMed]
20. Hřebíčková, M.; Jelínek, M.; Květon, P.; Benkovič, A.; Botek, M.; Sudzina, F. Big Five Inventory 2 (BFI-2): Hierarchický models 15 subškálami. *Československá psychologie* **2020**, in print.
21. Soto, C.J.; John, O.P. Short and Extra-Short Forms of the Big Five Inventory-2: The BFI-2-S and BFI-2-XS. *J. Res. Personal.* **2017**, *68*, 69–81. [CrossRef]
22. Sudzina, F.; Novak, R.; Pavlicek, A. *Impact of Personality Traits and Gender on Experiencing Virtual Offenses*; Doucek, P., Chroust, G., Oskrdal, V., Eds.; Trauner Verlag: Linz, Austria, 2018; Volume 47, ISBN 978-3-99062-339-8.
23. McCullagh, P. Regression Models for Ordinal Data. *J. R. Statistical Soc. Ser. B (Methodol.)* **1980**, *42*, 109–142. [CrossRef]
24. Aluja, A.; García López, O.; Garcia, L. Relationships among Extraversion, Openness to Experience, and Sensation Seeking. *Personal. Individ. Differ.* **2003**, *35*, 671–680. [CrossRef]