INFLUENCE OF ONLINE ROUTINE ACTIVITIES ON ONLINE PURCHASE FRAUD VICTIMIZATION

AN ANALYSIS OF THE SPECIAL EUROBAROMETER SURVEY 2018

EILEEN DEYHLE

Degree Project in Criminology
Master Thesis 15 Credits One-year master Criminology
11 / 2022

Malmö University
Faculty of Health and Society
205 06 Malmö

INFLUENCE OF ONLINE ROUTINE ACTIVITIES ON ONLINE PURCHASE FRAUD VICTIMIZATION

AN ANALYSIS OF THE SPECIAL EUROBAROMETER SURVEY 2018

EILEEN DEYHLE

Deyhle, E. Influence of online routine activities on online purchase fraud victimization. An analysis of the Special Eurobarometer 2018. *Degree project in Criminology 15 Credits.* Malmö University: Faculty of Health and Society, Department of Criminology, 2022.

Abstract: This paper uses Routine Activity Theory to examine online routine activities and individual level guardianship and the impact on online purchase fraud victimization across Europe. The findings suggest differences between the EU member states in online purchase fraud victimization. Moreover, it discovers that several online routine activities rise the victimization rate. However individual level guardianship has no great success in reducing victimization rates.

Keywords: criminology, cyber-crime, victimization, routine activity theory

Table of contents

Introduction

The invention and growth of the internet opened a whole new virtual world parallel to our real environment and enabled great opportunities for people to improve their lives. With the world-wide-web it is possible to keep realtime contact over large distances at low costs, shop online at every time, work or study from home, or even process official administrative procedures with citizen matters thanks to online identification systems. However, fast and great advancements in technology pave the way not only for lawful persons and businesses, but also for criminal activities and offenders who quickly adapt their methods to these changes. Online-chatrooms and social media that became popular among all age groups in the past years enable criminal activities such as child-pornography, catfishing, and online-grooming (Hernández et al., 2020). Other criminal activities performed in cyber space include illicit drug trade, mostly performed via the darknet, hacker attacks, malware, banking fraud, fraud with cryptocurrencies (van Wilsem 2013) All these criminal online activities can be condensed as *cyber crime*.

Especially during the Covid-19 pandemic the role of the internet increased exponentially and therefore the opportunities for online offenders (Cook et al., 2022). In the past years online crime rates have increased more than offline rates across Europe (Cook et al. 2022; Buil-Gilet al. 2021). In the UK in 2021, fraud and computer misuse happened more than twice the amount of thefts, burglaries, and robberies combined (UK ONS 2022). Since the internet and therefore cybercrime are international phenomena and offenders or offending groups act transnational it is of great importance to research and analyse this topic in an international context. To collect valuable, reliable and comparable data in different countries there are several surveys conducted within members of the European Union (EU), asking the same questions to a representative amount of inhabitants of the EU member states. One of these Surveys is the "Eurobarometer", a series of public opinion surveys requested by the European Commission and other EU institutions since 1973. The Special Eurobarometer Survey includes supplementary questions on special topics such as opinions, concerns, or experiences with cybercrime and cyber security (GESIS, 2020). The most recent Eurobarometer with information on cybercrime was collected in 2018 and offers a good possibility to analyse cybercrime and its influence factors in combination with various sociodemographic features.

One great approach to investigate online victimization is the Routine Activity Theory, since it is a salient theory on victimization (Holt & Bossler 2008; Reyns 2013; Leukfeldt & Yar 2016). Only a limited number of research has investigated this approach in combination with solely online routine activities. This paper focuses on the experience of victimization of online purchase fraud across European member states. The aim of the study is to examine individual patterns of internet use such as online banking, online purchasing, online selling, social networking, and emailing and their impact of the victimization rates of online purchase fraud. Additionally, individual level guardianship measures and their effect of victimization rates will be examined. The theoretical framework for this study is the Routine Activity Theory by Cohen and Felson (1979). The Special Eurobarometer on cybercrime from 2018 will be used as database.

The next section presents the theoretical background of this paper and previous research in the field of cybercrime. Subsequently the methodology and operationalization of this study will be presented prior to the results of the

analysis. Finally, the results will be discussed in the criminological context and this paper concludes.

Ethical considerations

This study is using official data provided by the Leibniz Institute for Social Sciences (GESIS). The data is openly accessible for the public to use in research papers like Master theses. The dataset contains personal information about the participants. Every person that participated has been anonymized and there is no possibility to trace back or harm the participants. Since this is official data there is no need to apply in front of the Faculty Ethic Council.

Theoretical Approach

The Routine Activity Theory developed by Cohen and Felson is a central approach in the field of criminology (Cohen & Felson, 1979). According to Routine Activity Theory, three conditions are necessary to create crime: (1) the presence of a motivated offender, (2) the availability of a suitable target that is vulnerable because of their risky routine activities, and (3) the absence of capable guardianship (Cohen & Felson, 1979). A person's activities and daily routines brings them into contact with motivated offenders and have an impact on the risk of victimization (Cohen & Felson 1979). Four dimensions seen from the offender's view influence a target's risk of victimization: (1) value, (2) inertia, (3) visibility, and (4) access (Cohen & Felson 1979).

Routine Activity Theory has been widely researched in criminology in the offline world, but there is scepticism among researchers when Routine Activity Theory is applied to the cyber space. While some researchers distinguish the cyber world from the terrestrial world, and suggest a transformation of scientific assumptions among criminology. They see cyber crime as a new phenomenon with a new space. Others suggest to continue with the elements of theories and simply apply offline concepts to online phenomena and view cyber criminality as basically the same as terrestrial criminality (Leukfeldt & Yar, 2016). After a systematic theoretical reflection, Yar (2005) concludes that the concepts of motivated offender and capable guardianship can be treated relatively similar between offline and online settings. He applied the core elements of Routine Activity Theory (motivated offender, suitable victim, capable guardian) to the online environment. It was no problem to prove that there is a mass of motivated offenders across the internet, such as hackers, stalkers and fraudsters. Suitable targets share personal information, use online-payments, or conduct purchases. Capable guardians across the internet include administrators, users, peers, but also technology, such as firewalls, antivirus software, or private networks (Yar, 2005). However, the "cyber-space is spatio-temporally *disorganized*" (Williams 2016: 23) and victim and offender are rarely physically close to each other. According to Eck and Clarke (2003) the necessary "shared physical space" can be expanded to a "shared network", such as the internet, where the offender can reach his target through this network.

Internet use frequency, or online activity measures the suitability of the target, while guardianship is measured by cybersecurity management (Lee & Wang, 2022). Routine Activity Theory provides a framework to examine a victim's characteristics to understand victimization in cyberspace (Leukfeldt & Yar, 2016).

This theoretical approach states that cybercrime is enabled by computer networks linking motivated offenders with suitable victims in the absence of capable guardianship. To apply Routine Activity Theory to victimization of online purchase fraud the elements need to be clear. Online purchase fraud in this paper is considered as purchasing a good via the internet but not receiving it. A motivated offender is the fraudster who pretends to sell goods in online shops. A suitable target is the person who wants to buy the good and conducts a transaction believing to receive something for their money. The capable guardian that is lacking in order to enable crime can be software to detect untrustworthy websites or suspicious bank account transactions.

Previous Research

Several studies have examined Routine Activity Theory in combination with cybercrime. Using the British Crime Survey (08/09), Reyns (2013) showed that parts of Routine Activity Theory, such as using the internet for banking, shopping emailing or downloading, were related to identity theft. Reyns and Henson (2015) examined the Canadian General Social Survey and found that online banking and purchasing influence the likelihood of being a victim to identity theft. A study on Internet consumer fraud conducted by van Wilsem (2013) showed that online purchasing and using online forums increased the victimization of cybercrime. Williams (2016) conducted the first multilevel cross-national study on cybercrime victimization and was the first that focused exclusively on online identity theft. He discovered that online routine activities like auction selling and accessing in public places increased the probability of online identity theft in Europe. He examined individual levels of guardianship and their association with online identity theft, and the interaction with country-level guardianship. He showed that country-level guardianship, such as internet infrastructure, or national cybersecurity measures moderate the effectiveness of individual-level guardianship and on reducing the probability of inline identity theft (Williams, 2016).

The research linking Routine Activity Theory to online identity theft grew in the past years, however, the evidence base for other cybercrimes is less developed. According to Holt and Bossler (2008) and van Wilsem (2011) physical guardianship, such as using antivirus software, was not associated with cyber-harassment. Bossler and Holt (2009) showed that personal and physical guardianship were unrelated. However, their study had significant limitations because they used college student populations as sample which could have inevitable biases. A study from the Netherlands showed that some parts of Routine Activity Theory are associated with different cybercrimes, while technological guardianship show a less clear relationship (Leukfeldt & Yar, 2016). Lee and Wang (2022) used a multilevel latent class analysis of data from the 2019 Eurobarometer to analyse individual level and country-level patterns of cybercrime victimization. Their findings suggest that there are two overarching victim profiles across Europe.

Based on the theoretical framework of Routine Activity Theory and the previous research this paper will try to examine the association between activity patterns, effects of guardianship and the risk of victimization in the cyber space in Europe and. The specific cybercrime analysed will be online purchasing fraud. Previous studies that used similar databases created three types of individual guardianship (Williams 2016; Cook et al. 2022). Changing security settings and using different passwords for different websites are viewed as active guardianship since the

individual is putting active effort in protection from cybercrime. Rejecting unknown emails, only using their own computer and trusted websites, and installing antivirus software is considered as passive guardianship because these are things that happen in the background. Only using trusted computers and websites is done automatically without thinking about it. An existing antivirus software runs in the background and is protecting the user without noticing or activating it each time of use. Finally, reducing the use of the internet for activities like banking, purchasing, or selling counts as avoidance guardianship, because the user avoids the internet, maybe because he or she has already made experiences with cybercrime.

Because of the limited frame of this thesis, this paper will only focus on individual-level guardianship, such as active, passive, and avoidance guardianship explained above. This leads to the following Hypotheses:

H1: rates of victimization of online purchase fraud varies within European countries

H2: Internet use patterns are positively associated with victimization of online purchase fraud

H3: individual level guardianship is negatively associated with victimization of online purchase fraud

The second hypothesis tests the application of Routine Activity Theory on online purchase fraud. Following the work of van Wilsem (2013) and Reyns (2013) the third hypothesis tests the association between online purchase fraud and individual level guardianship.

Methodology

Dataset

This paper uses data from the Special Eurobarometer survey on Cybersecurity collected in 2018 and commissioned by the European Commission. The Special Eurobarometer is part of the Standard Eurobarometer Survey, conducted bi-annually since 1973, and is the largest and most comprehensive survey on cybercrime globally, that statistically represents the domestic population in Europe. The data was collected between October and November in 2018 in all 28 EU Member States (including the now departed UK) via face-to-face interviews in the respondents' homes. The survey had a total number of observation of 27607 particpants that were analysed after weighting the sample proportional to population size of each country. The item non-response was less than two per cent. The GESIS Leibniz Institut (2020) provides further details about the Eurobarometer Survey.

Operationalization

The dependent variable in this study is experience of online purchasing fraud. This kind of victimization is measured by the question if the participant has had experiences with victimization of online purchasing fraud in the past three years. The item had five response categories according to the frequency of reported victimization: 1 = once; 2 = two or more times; 3 = more than three times; 4 = never; and 5 = don't know. This variable was recoded into the categories 0 = never; 1 = occasionally; 2 = often. The fifth response category was coded as missing data. After exploring, this variable showed an extreme positive skew with

a majority not experiencing purchasing fraud victimization, and the minority experiencing at least one time of online purchase fraud. Linear regression models are not fitting to such distributions, and a multi-nominal does not fit for the order of the categories which are important to account for repeat victimization (Williams, 2016). The fact that this dependent variable needs more categories to show the increased risk of victimization also cuts out the possibility of a binary coding and therefore a logistic regression. The distance between response items is not equal, which is why ordinal regression is not appropriate in this case. Poisson models are suiting for this kind of data because they recognize crime rates on counts of crimes (see Williams 2016; Osgood 2000).

The independent variables on the individual level include online routine activities, internet use frequency, guardianship and sociodemographic factors.

To assess online routine activities the participants were asked if they had engaged in several online activities in the past 12 months including banking, purchasing, selling, social networking, or emailing. These variables were scaled as binary covariates with the values: 0 = no; 1 = yes; because high values and therefore engaging in online activities is expected to indicate a high probability of victimization (Field 2017).

The internet use frequency was measured through the question how often the participant uses the internet at home, at work, on a mobile device, or elsewhere. These variables were computed to a scale covariate ranging from 0 to 12. The cronbach's alpha was at 0,78 (see Field 2017).

To examine individual-level security measures participants were asked whether their concerns about security issues made them change the way they used the internet. The dataset has 15 items in total to assess this question on which Exploratory Factor Analysis (EFA) was performed. This resulted in three main factors with eight variables in total which can be, following previous research that adjusted capable guardianship (Williams 2016), described as active guardianship (changing security settings and using different passwords for different websites), passive guardianship (less online purchases and less online banking), and avoidance guardianship (rejecting unknown email, only using own computer, only visiting trusted websites, and installing antivirus software). The items were computed to the respective factors and the values were recoded to binary categories: 0 = yes, changed something; 1 = no, did not change anything. This coding is consistent with the assumption that high values indicate higher risk of victimization.

This study also includes sociodemographic variables, such as gender, age, community size, and social status. Gender is a binary variable with 0 = male; and 1 = female. Age is divided into 4 categories with lower values indicating lower age. Community size is assessed through the question in what area the participant is living, with values 0 = urban and suburban area; and 1 = rural area. Individuals were asked to self estimate their own social status, and this is used in a continuous variable with the values 0 = working class; 1 = lower middle class; 2 = middle class; 3 = upper middle class; 4 = upper class.

Analytic Strategy

After drawing the descriptive statistics on the variables, a multi-level Poisson regression analysis with will be conducted to show the variables' impact on

variations of experiencing online purchase fraud. The descriptive and regression models were conducted via SPSS (IBM).

Results

Table 1 (see appendix) shows the incidents of online purchase fraud in a population weighted sample across the EU member states. The victimization rates vary across the countries with the majority of people never experienced online purchase fraud in the past 12 months. This confirms Hypothesis H1.

Table 2 (see appendix) provides the descriptive statistics for the dependent and the independent variables. 14 variables were included in the analyses, and three variables have no missing values out of the total number of observations of 27607. The other variables show a missing data of between 767 and 4575. Gender has a mean of 0.52 indicating slightly more females in the sample. The dependent variable experience of online purchase fraud shows a skewness of 2.898 indicating a Poisson distribution.

The next section shows the results from the multi-level Poisson regression analysis with experience of online purchase fraud as dependent variable. The continuous variable information shows a mean of 0.149 and a variance of 0.166 for the dependent variable which is a ratio of 0.166/0.149 = 1.11. A Poisson distribution requires the mean and variance to be equal, meaning a ratio of 1 (Osgood 2000). In this case, there is a small amount of overdispersion, which will be discussed later. To check if the model fits to the data, the table for Goodness of Fit (see appendix), shows a Pearson Chi-Square of 1.104, which indicates, again, a slight overdispersion. The omnibus test has a p-value of 0.000 showing that the model is significant. Model 1 with the individual- level covariates, indicates the extent to which demographic poperties and internet use patterns influence variation in the event of online purchase fraud (Table 5). Most of the online routine activities are significantly predictive of online purchase fraud, which supports partly hypothesis H2. Looking at the exponentiated B coefficient of online activity purchasing shows that the victimization rate will be 1.33 times or 13 per cent greater for those using the internet to purchase things given that all other factors are held constant. A similar outcome shows online selling with approximately 14 per cent higher rates of victimization for those selling goods on the internet. Online banking activities were not significant in this study. Social networking and emailing have a negative association with victimization, which indicates that not following those activities might increase the victimization rate. The Exp(B) of Internet use frequency states that an increase of one unit will increase the victimization rate by 1.047 or 10.4 percent.

Looking at demographic statistics shows negative B coefficients for age. Increased age indicates less victimization given the fact that the other variables are held constant. For example, compared to the reference age group (15 – 24 years) being in the age group 25-39 will increase the victimization rate by 8.35 per cent. Having working class as reference variable for social status, the results show a victimization rate 1.32 times higher for people that self-assessed as lower middle class. Result on the upper class were not significant. Living in a rural area is negatively associated with victimization of online purchase fraud and has a 0.9 times greater victimization rate than not living in a rural area. Finally, gender is also significantly associated with victimization showing an Exp(B) of 0.854. This indicates that being a female increases the victimization rate by 8.5 percent given that all other factors are held constant.

Adding variables of active, passive and avoidance guardianship in model 2 create a very small change to the previous independent variables from model 1. The social upper class and online banking stay not significant while the Exp(B) value for almost all other variables decreased very slightly. Given that all other factors are held constant, not using active guardianship (changing security settings and passwords) or avoidance guardianship (less purchases, less online banking) indicates a purchase fraud victimization rate of 0.72. Passive guardianship (rejecting unknown email, using only the own computer, visiting only trusted websites, installing antivirus software) as influence factor is not significant in this model. Active and avoidance guardianship are negatively associated with victimization of online fraud which supports Hypothesis H3.

Discussion

The aim of this paper was to explore the influence of several individual-level factors on victimization of online purchasing fraud across Europe using Routine Activity Theory. The study reveals that online routine activities such as online purchasing, selling, social networking, emailing, and internet frequency use are significantly associated with victimization rates. Email use and social networking have a negative association with victimization of online purchase fraud indicating that those who do not use email have higher victimization rates. Williams (2016) had a similar outcome and conducted an additional logistic regression to examine this phenomenon. His analysis revealed that individuals that do not use email were more likely to be aware of cybercrime and avoid online activities. That could be a possible explanation for the findings in the current study.

The sociodemographic factor age is negatively associated with the outcome variable indicating that a decrease of every unit age (years) will increase the victimization rate. This leads to the assumption that the older an individual is the higher is their risk of being a victim to online purchase fraud. However, this needs to be investigated further in the future to explore the mechanisms of online purchase fraud in association with age. The findings could help to increase cyber-security for elderly, and protect them from victimization.

Adding individual-level guardianship to the analysis decreased the influence of the previous variable only slightly. This indicates that individual guardianship measures such as changing security settings and passwords, rejecting unknown email, using only the own computer, visiting only trusted websites, installing antivirus software, purchase less online, and conduct less online banking do not solely save a person from becoming a victim of online purchase fraud. This suggests that there are other measures that fit better to avoid victimization, probably on the country-level. Williams (2016) tested also for country-level measures such as national cyber-security strategies and development of internet infrastructure and showed that these factors moderate individual passive guardianship with higher effectiveness in higher developed countries (in terms of internet and cyber security). Since this is the first study that focuses solely on online victimization of identity theft the results are not universally applicable and needs further research and validation (Williams 2016). However, his study focuses on identity theft and the individual level guardianships fit well to this kind of cyber-crime. In the current paper, passive guardianship showed no significant influence on online purchase fraud. This could be due to the fact that the victimization of purchase fraud includes purchasing a good and not receiving it. Passive guardianship measures consist of rejecting unknown email, only using the own computer, visiting only trusted websites, and using antivirus software. Those

are not very capable to prevent someone from not sending a package. For future research different, better fitting guardianships will be needed.

This study could not examine country-level guardianship which could have a great impact on online purchase fraud. Controlling and prosecution mechanisms by the government could decrease and prevent victimization of purchasing fraud. Especially in the Covid-19 pandemic the number of online purchases increased extremely, because everyone stayed at home (Young et al., 2022). This creates a great opportunity for offender to fraud in selling goods. However, the dataset for this current paper is a survey from 2018, before the pandemic, and does not show this pattern. Future studies should focus on that aspect, understanding the associations can help create capable country-level guardianship.

The analysis showed an overdispersion of the Poisson model. Poisson regression requires an equation of the mean and the variance which was not fulfilled in this study. Within the format of this thesis the problem of overdispersion is left out for this analysis. When conducting an actual study that is acknowledged, this problem needs to be addressed and fixed, e.g. by using a non-binominal negative regression (Osgood, 2000).

The results could confirm the hypotheses that link Routine Activity Theory and individual level guardianship to victimization rates of online purchase fraud, even though individual level guardianship has no great impact on decreasing victimization rates. The Routine Activity Theory is a great approach for further research.

Conclusion

The current paper connects one of the most important theories in the field of criminology, the Routine Activity Theory, to a relatively new type of crime, happening solely in the online world. The study shows that a theory that was created offline, before the existence of the internet, is timeless and can be applied to all new developments in the world, such as completely online crimes. The findings in this study show an association between individual factors and internet use habits and cybercrime in Europe, but have no great impact. Other studies take a step forward and investigate capable guardianship measurements on the macro-level and have more satisfying results. This indicates the right direction of research and should be further investigated in the future.

This study used a Poisson regression model to estimate victimization rates of online purchase fraud across Europe in 2018, which has not been examined before in that way. As stated before, more interesting result could be found in later Surveys, considering the Covid-19 pandemic and the change of internet use and online purchase habits of individuals. However, this study shows several limitations that have been addressed and need to be avoided in the future.

Literature

Bossler, A. M., & Holt, T. J. (2009). On-line Activities, Guardianship, and Malware Infection: An Examination of Routine Activities Theory. *International Journal of Cyber Criminology*, *3*, 400-420.

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies*, *23*(sup1), S47-S59. https://doi.org/10.1080/14616696.2020.1804973

Cohen, L. E., & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review*, *44*(4).

Cook, S., Giommoni, L., Trajtenberg Pareja, N., Levi, M., & Williams, M. L. (2022). Fear of economic cybercrime across Europe: A multilevel application of Routine Activity Theory. *The British Journal of Criminology*. https://doi.org/10.1093/bjc/azac021

Eck, J. E., & Clarke, R. V. (2003). Classifying Common Police Problems: A Routine Activity Theory Approach. *Crime Prevention Studies*, *16*, 33.

European, C., & European Parliament, B. (2021). Eurobarometer 92.2 (2019). In: GESIS Datenarchiv, Köln. ZA7580 Datenfile Version 1.0.0, https://doi.org/10.4232/1.13657.

Field, A. (2017). *Discovering Statistics Using IBM SPSS Statistics*. SAGE Publications.

GESIS Leibniz Institut für Sozialwissenschaften. (2020). *GESIS - Leibniz Institute for the Social Sciences.* https://www.gesis.org/en/eurobarometer-data-service/survey-series/standard-special-eb/sampling-and-fieldwork (Last visited 04.11.2022).

Hernández, M. P., Schoeps, K., Maganto, C., & Montoya-Castilla, I. (2020). The risk of sexual-erotic online behavior in adolescents – Which personality factors predict sexting and grooming victimization? *Computers in Human Behavior*, *114*. https://doi.org/10.1016/j.chb.2020.106569

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

IBM Corp. Released 2021. *IBM SPSS Statistics for Windows,* Version 28.0. Armonk, NY: IBM Corp

Lee, C. S., & Wang, Y. (2022). Typology of Cybercrime Victimization in Europe: A Multilevel Latent Class Analysis. *Crime & Delinquency*, 28. https://doi.org/10.1177/00111287221118880

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

Office for National Statistics (ONS), released 26 September 2022, ONS website, article, Nature of fraud and computer misuse in England and Wales: year ending March 2022

https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022 (last visited: 04.11.2021)

Osgood, D. W. (2000). Poisson-Based Regression Analysis of Aggregate Crime Rates. *Journal of Quantitative Criminology*, *16*(1), 21-43. https://doi.org/10.1023/A:1007521427059

Reyns, B. W. (2013). Online Routines and Identity Theft Victimization:Further Expanding Routine Activity Theory beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, *50*(2), 216-238. https://doi.org/10.1177/0022427811425539

Reyns, B. W., & Henson, B. (2015). The Thief With a Thousand Faces and the Victim With None: Identifying Determinants for Online Identity Theft Victimization With Routine Activity Theory. *Int J Offender Ther Comp Criminol*, *60*(10), 1119-1139. https://doi.org/10.1177/0306624X15572861

van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology*, *8*(2), 115-127. https://doi.org/10.1177/1477370810393156

van Wilsem, J. (2013). Hacking and Harassment—Do They Have Something in Common? Comparing Risk Factors for Online Victimization. *Journal of Contemporary Criminal Justice*, *29*(4), 437-453. https://doi.org/10.1177/1043986213507402

Williams, M. L. (2016). Guardians Upon High: An Application of Routine Activities Theory to Online Identity Theft in Europe at the Country and Individual Level. *British Journal of Criminology*, *56*(1), 21-48. https://doi.org/10.1093/bjc/azv011

Yar, M. (2005). The Novelty of 'Cybercrime':An Assessment in Light of Routine Activity Theory. *European Journal of Criminology*, *2*(4), 407-427. https://doi.org/10.1177/147737080556056

Young, M., Soza-Parra, J., & Circella, G. (2022). The increase in online shopping during COVID-19: Who is responsible, will it last, and what does it mean for cities? *Regional Science Policy & Practice*. https://doi.org/10.1111/rsp3.12514

Appendix

Table 1: Crosstabulation of online Purchase Fraud in Europe

	Experience of online purchase fraud			
	Never	Occasionally	Often	Total
AT - Austria	343	55	10	408
BE - Belgium	456	74	13	543
BG - Bulgaria	248	18	4	270
CY - Cyprus (Republic)	32	4	0	36
CZ - Czech Republic	392	64	14	470
DE-E Germany East	630	87	16	733
DE-W - Germany - West	2753	394	49	3196
DK - Denmark	258	32	4	294
EE - Estonia	51	6	1	58
ES -Spain	1970	118	12	2100
FI - Finland	235	23	3	261
FR - France	2558	369	60	2987
GB - United Kingdom	2682	370	62	3114
GR - Greece	413	19	0	432
HR - Croatia	150	22	11	183
HU - Hungary	355	35	24	414
IE - Ireland	186	23	3	212
IT - Italy	2401	244	77	2722
LT - Lithuania	102	8	2	112
LU - Luxembourg	24	4	0	28
LV - Latvia	76	9	1	86
MT - Malta	15	3	0	18
NL - The Netherlands	767	127	10	904
PL - Poland	1366	124	25	1515
PT - Portugal	393	11	1	405
RO - Romania	619	64	27	710
SE - Sweden	444	64	6	514
SI - Slovenia	76	9	1	86
SK - Slovakia	205	14	2	221
Total		20200	2394	438

Weighted population sample

Table 2: Univariate descriptive statistics

	N						
	Valid	Missing	Mean	Std. Deviation	Skewness	Minimum	Maximum
Experience of online purchase fraud	23032	4575	0,14	0,399	2,898	0,00	2,00
Gender	27607	0	0,52	0,499	-0,062	0,00	1,00
Age	27607	0	1,91	1,058	-0,461	0,00	3,00
Size of community	27607	0	0,24	0,426	1,231	0,00	1,00
Social status	26840	767	1,39	0,982	-0,167	0,00	4,00
Online activity: Banking	23420	4187	0,61	0,488	-0,445	0,00	1,00
Online activity: Purchasing	23420	4187	0,55	0,498	-0,194	0,00	1,00
Online activity: Selling	23420	4187	0,22	0,416	1,337	0,00	1,00
Online activity: social networking	23420	4187	0,62	0,486	-0,488	0,00	1,00
Online activity: Email	23420	4187	0,80	0,402	-1,475	0,00	1,00
Internet use frequency	24240	3367	6,96	3,850	-0,534	0,00	12,00
Active guardianship	23420	4187	0,66	0,475	-0,656	0,00	1,00
Passive guardianship	23420	4187	0,28	0,451	0,957	0,00	1,00
Avoidance guardianship	23420	4187	0,85	0,362	-1,906	0,00	1,00

Table 3: Goodness of Fit

	Value	df	Value/df
Deviance	11237,012	18799	,598
Scaled Deviance	11237,012	18799	
Pearson Chi-Square	20795,217	18799	1,106
Scaled Pearson Chi-Square	20795,217	18799	

Dependent Variable: new experience of purchase fraud

Table 4: Omnibus Test[a]

Likelihood Ratio Chi-Square	df	Sig.
453,186	15	,000

Dependent Variable: new experience of purchase fraud
Model: (Intercept), gender_new, age_new, sizeofcommunity_new, socialclass_new, new_banking_onlineactivities, new_purchasing_onlineactivities, new_selling_onlineactivities, new_socialnetwork_onlineactivities, new_email_onlineactivities, Internet_Use_Freq

a. Compares the fitted model against the intercept-only model.

Table 5: Poisson regression analysis

	Model 1					Model 2				
	B	SE	Exp(B)	95% Wald CI for Exp(B)		B	SE	Exp(B)	95% Wald CI for Exp(B)	
				Lower	Upper				Lower	Upper
(Intercept)	-1,974	0,10	0,139	0,114	0,169	-1,391	0,12	0,249	0,198	0,313
Sociodemographics										
Gender - Female	-0,16**	0,04	0,854	0,792	0,920	-0,16**	0,04	0,852	0,790	0,918
reference: male gender										
Age: over 55 years	-0,53**	0,07	0,587	0,512	0,673	-0,56**	0,07	0,573	0,500	0,658
Age: 40 - 54 years	-0,26**	0,06	0,770	0,689	0,860	-0,28**	0,06	0,759	0,679	0,848
Age 25 - 39 years	-0,18**	0,06	0,835	0,750	0,930	-0,18**	0,06	0,833	0,748	0,928
reference: age 15 - 24 years										
community	-0,11*	0,05	0,893	0,812	0,982	-0,10*	0,05	0,902	0,820	0,992
reference suburban and urban										
Social status: upper class	-0,03	0,19	0,973	0,664	1,426	-0,11	0,20	0,898	0,613	1,316
Social status: upper middle class	0,29**	0,08	1,332	1,149	1,545	0,27**	0,08	1,311	1,130	1,521
Social status: middle class	0,17**	0,05	1,188	1,072	1,316	0,17**	0,05	1,184	1,068	1,311
Social status: lower middle class	0,28**	0,06	1,320	1,166	1,493	0,27**	0,06	1,308	1,156	1,479
reference: working class										
Online routine activities										
Banking	0,09	0,05	1,097	0,996	1,208	0,09	0,05	1,101	0,999	1,213
Purchasing	0,28**	0,05	1,325	1,206	1,455	0,25**	0,05	1,284	1,167	1,411
Selling	0,36**	0,04	1,437	1,322	1,563	0,34**	0,04	1,398	1,286	1,520
Social networking	-0,13**	0,05	0,880	0,807	0,960	-0,14**	0,05	0,871	0,798	0,950
Email	-0,49**	0,05	0,612	0,551	0,681	-0,53**	0,06	0,589	0,529	0,655
Internet use frequency	0,05**	0,01	1,047	1,030	1,064	0,04**	0,01	1,041	1,024	1,059
Capable guardianship										
Active guardianship						-0,33**	0,04	0,718	0,663	0,778
Passive guardianship						0,05	0,05	1,047	0,959	1,143
Avoidance guardianship						-0,33**	0,05	0,719	0,652	0,792

Dependent Variable: experienced online purchasing fraud; *p < 0.05; **p < 0.01