CRIME PREVENTION- HOW TO AVOID SUBSCRIPTION TRAPS

Vesa Hietanen
Laurea University of Applied Sciences, Research, Innovative Digital Services of the Future, Finland
European Cyber Crime and Fraud Investigators
www.eccfi.eu
vesa.hietanen@yahoo.com

ARTICLE INFORMATION

Article History:
Received Sept 19, 2017
Revised Oct 31, 2017
Accepted Oct 2, 2017

JEL Classifications
G23; I22; K14

Key Words:
Cybercrime,
subscription traps,
digitalization, phishing,
payments,
legislation

DOI:
10.21532/apfj.001.18.03.02.06

ABSTRACT:
In Europe, 3.5 million consumers are estimated to have been affected by subscription traps over the past three years. This is more frequently the case now than ever before due to digital evolution which offers more opportunities to communicate and gather information from consumers. Subscription traps are offers on cheap products that lead to costly subscriptions for those who accept them. Usually, the consumer needs to pay with a debit or credit card to claim the offer. Although each free trial should be examined on a case-by-case basis, some practices are considered illegal upfront. Subscription traps include practices that are breaches of EU law or include grey zone practices that push the boundaries of what is legal or are currently untested by EU law.

This case study focuses on two research questions: 1) what circumstances creates subscription traps? and 2) how do we fight against them? A survey was conducted to professionals who had experience in subscription traps and cybercrime. The respondents (n=73) consisted of lawyers, prosecutors, police officers, risk specialists, payment card specialists, credit managers and product specialists from 14 countries. Furthermore, two individuals who did not participate in the survey were interviewed.

Research findings explain why the phenomenon of subscription traps has exploded exponentially in Europe. Furthermore, the study suggests that in the prevention of such traps the police should have better tools and methods for pre-trial investigations and charges should be made to criminals for customer manipulation and misrepresentation. Support, awareness, and education should be focused on the individuals whose digitalization skills are not on a par with the majority.

This case study concludes that legislative changes should be made. Legislation should include clear penalties based on

legal practices through which the activities of the responsible parties behind these subscription traps can be shut down. The authorities and the private sector should consider forms of cooperation in order to enhance the prevention of such crime. Additionally, it was found out that for a large number of authorities and financial representatives, the kind of crime to which subscription traps belong remained unclear.

1. Introduction

Business intelligence provides consumers with new digitalization tools to facilitate everyday life (eg. payments) and thus provide added value for such services. In making fast and easy online transactions, the importance of security should be kept in mind. Criminals learn very quickly new technology and are capable of recognizing loopholes necessary to carry out their crimes. The internet is increasingly used by cyber criminals to develop new methods and to conceal such methods in the execution of their fraudulent plans.

Based on research, subscription traps actually began in Finland and elsewhere in Europe back in 2011-2012. According to Caroline Theorell's (2017) survey, subscription traps have caused a lot of problems for consumers, financial institutions and authorities over the years. Subscription traps typically and entirely exist online, a so-called "cross-border crime". A subscription trap means that the consumer receives invoices for a product or service that he has not ordered for himself. This, in turn, leads to a deliberate misrepresentation to the consumer as the consumer does not receive a real image of the advertiser or the message. In the electronic world, media literacy means how the recipient can filter information and evaluate its quality. Media literacy also refers to the ability to understand what kind of choices have been made in the information content, who has produced the information and what is left unrecognized.

2. Background

The Internet has, over time, increasingly intertwined with the lives of Finns as more and more essential products and services are available online. According to Statistics Finland, around 90% of the population aged 16 to 74 practically "live on the internet" and around 70% use the Internet several times a day. Although the average Internet usage is generally lower in the older generation, a significant 30% of people aged 65-74 (or more than 200,000 of the population), use the Internet several times a day.

With the rise of Internet usage over time and its interconnection with individuals on a more personal level, so do the interest of online fraud and the cybercrime population increase. These cybercriminals are particularly interested in banking and payment transactions as well as electronic identification (Schmalleger and Pittaro, 2008).

With the growth of social media, new services continuously enter the market. Thus, social media usage largely reflects mobile usage. Nearly 95% of users of community services use Facebook and 10-20% use Twitter, LinkedIn and Instagram. However, these social media services have a great age distribution. Instagram is more popular among young people, while LinkedIn is aimed more at the working population. Nowadays the use of desktop devices have significantly lessened compared to the use of hand-held devices (eg. smartphones, tablets) especially in the younger generation. For example among individuals born in the year 1980 to 2000 in the United States, every fifth does not use internet anymore on computers (Ilmarinen and Koskela, 2015).

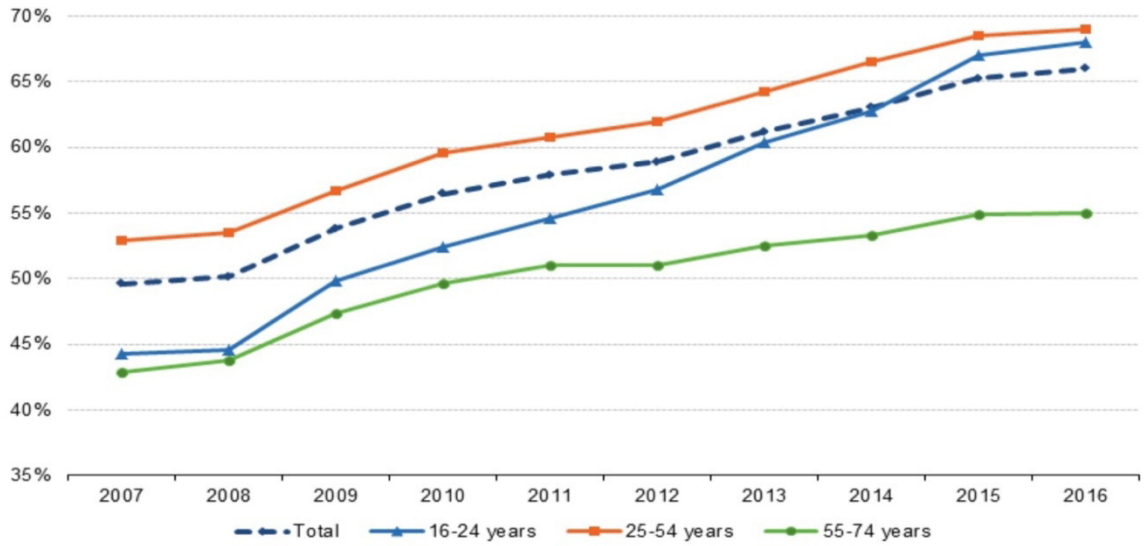

Figure 1: Consumers who bought goods or services through the internet (Eurostat 2017)

Security is important when talking about digitalization. There are threats in both the physical and the digital world, the elimination of which is seldom possible or rational. How a business handles security threats is affected by its anticipation and state of preparedness. (Ilmarinen and Koskela, 2015). For example, regulation of customer and personal data processing and PCI DSS card payment demands requirements on how to handle security issues in companies.

As a result of digitalization, new kinds of threats have emerged from both the social and service users' point of view. Digital services are based on openness when services and interfaces are available through open access. Data networks carry large amounts of information, as well as sensitive data in digital form (Ilmarinen and Koskela, 2015). Payments and other financial transactions are already well-digitized. In a networked society, safety is the result of co-operation between suppliers, contractors, partners and service ecosystems. Customers and users who are often the "weakest chain link" are usually added to the chain. (Limnéll et. Al. 2014)

In the information society as a whole, there are numerous opportunities as well as risks and threats - real and experienced. These dangers, however, are not created by technology or the internet but by the operators themselves. Problems and risks also arise from the fact that on the Internet the speed, scale and the ease of access to harmful information makes the community difficult to control. The Internet and the web, like any technology, are inherently worthless (Heinonen, 2009). When the information society is transformed into a new society where intelligent technology is present everywhere, the possibility of manipulation and abuse increases in the same proportion as the opening up of new opportunities to intercultural interaction in virtual communities (Heinonen, 2009).

In the light of these statistics, the fact that many subscription companies promote and market in social media is not surprising. In the case of subscriptions, Facebook becomes the number one site in social media, where these companies use targeted marketing. All companies that offer similar marketing to customers on the web are also possible sources of such crimes. Subscription ads and banners have also been found on well-known

newspapers in Finland, so any commercial site may be a potential subscriber banner distributor offering marketplaces for advertisers.

3. What circumstances creates subscription traps?

When something seems too good to be true, it is usually a scam. In the case of cheating for subscriptions, a one-euro payment is usually required to allow the consumer to enter his card information. The price of the product is really not relevant. The only goal is to get the consumer card information and thus get the card charged. When the customer enters the card information, the consumer agrees and accepts the terms under which a commitment is made to a one-time subscription. In general, it is very difficult to get rid of these service contracts and the process with which the customer can break free from it has been made very difficult (Nets, 2017). The product in question is never, or otherwise very rarely sent, and is often replaced with another substantially worthless product.

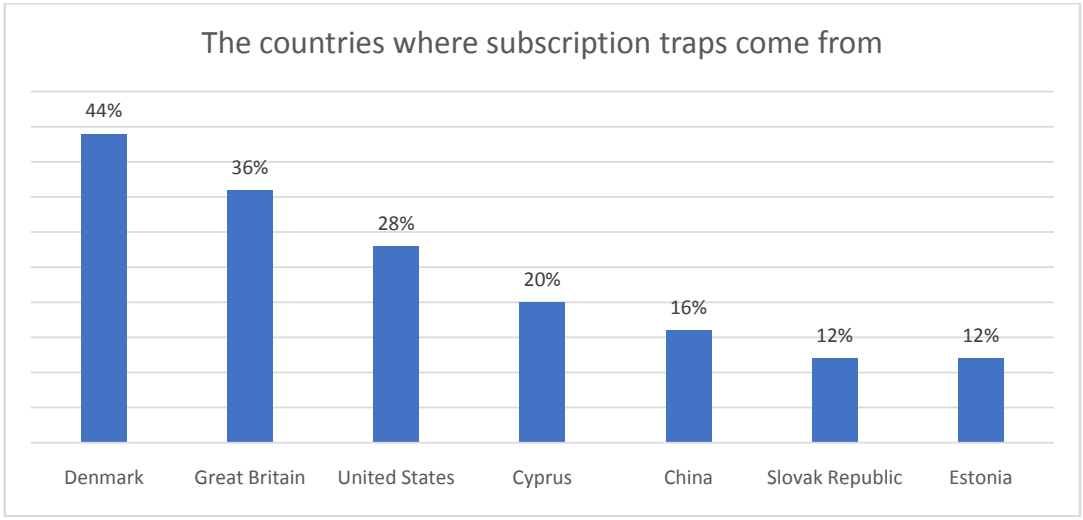

Figure 2: A survey was conducted to professionals who had experience in subscription traps and cybercrime .

Since 2012, subscription traps have been added every year. Some of the chargers would change the name of the company, but the mode of operation was always the same. Subscription traps began to affect European consumers first from the United States, which involved a lot of orders for cosmetics and especially for weight loss products. Very soon the phenomenon increased month after month, and scams from Denmark increased rapidly. The phenomenon also saw changes in products from physical products to digital services. This is partly because companies wanted to make their processes as flexible as possible and avoid chargeback orders. In particular, on Facebook, subscription scams initially were operated freely and their investigation was relatively difficult. In the qualifications, it was noticed that targeted ads appeared only to specific profiles (eg. female, retired, etc.) especially for older age groups.

Subscription trap scamming sights have already lured thousands of victims over time. This can also affect the quantity criminal reports, since most of the clients who have filed for complaints have also filed a criminal offense. On Facebook, websites that use product testers have given different offers as well. However in one of the cases I have investigated, the company Jobform.com was registered in the United Arab Emirates, but its IP address was registered in Thailand and consumer issues were handled under their own terms in Hong Kong.

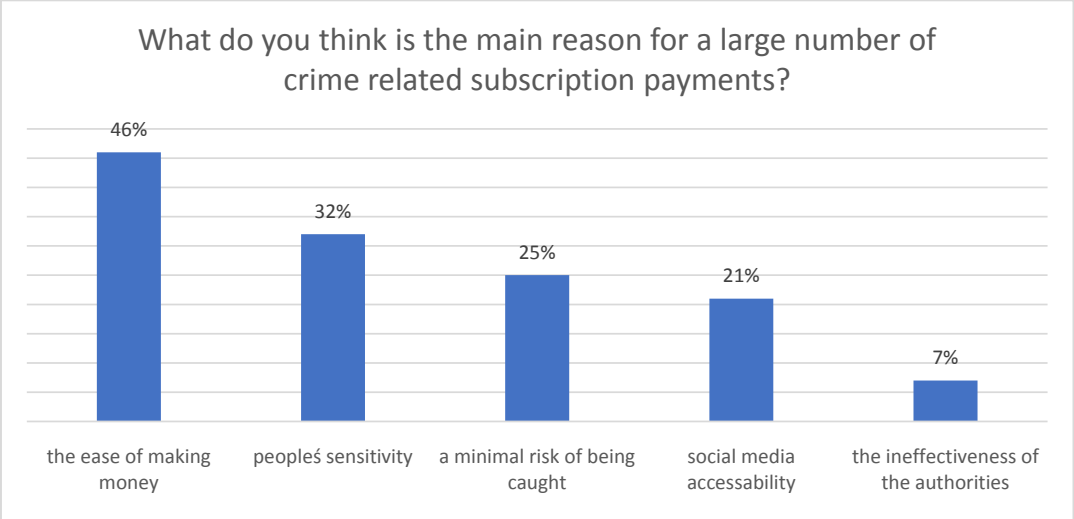

Figure 3: A survey was conducted to professionals who had experience in subscription traps and cybercrime.

A continuous charge is an order made on the internet, which is renewed periodically. For example, the service may include continuous access to a particular site or participation in a contest or poll. Usually, when an order is made, the customer is unaware of the existence and the commitment to a continuous charge. Continuous charging works so that a business charges a fee on a given card weekly, every 2 weeks, monthly, or even annually. The charging schedule is determined by the subscription service. If the order is canceled within the indicated deadline on the website, there will be no charge. The operating model is almost identical in all cases. For example, an advertisement on the Internet (eg. Facebook) or in one's email offers jogging shoes or slimming pills for the price of 2 euros (Enforcement and European Consumer Centres, 2016). In order to receive the item, one has to answer a questionnaire. Additionally, before answering the questionnaire, one must accept the small printed terms and provide his/her credit card details. Thus, the customer unknowingly subscribes to a monthly membership fee of 40-80 euros.

Subscription trap company WeKeepItSafe states in its terms that by accepting a charge, the customer will receive an experimental membership for a seven-day period at a price of 1.00 €. In addition, the customer accepts and the membership will be automatically renewed. Membership does not cost 1.00€ more for the first seven days, which is considered the probationary period. If the customer does not want to continue membership after this period, the membership must be canceled before the next payment date. After the test period expires, the membership costs 1.30€ per day and the customer is charged once a month (30 days with 39.00€) until the customer withdraws the membership. One of the cases I have investigated is a good example of how companies do not have the intention of sending customers any kind of one-euro product. In this company, the membership gift was an Android tablet and the customer joined on May 5, 2014. The link to redeem the gift was in a separate service (giftcable.com) and was reported via email. Subscription companies also attempt to disguise e-mail as spam to possibly target the consumer's spam folder. This is done so that the consumer would find it even more difficult to detect and respond to the email within a specified time.

8.5 documents approved by giftcable.com. The birth date had to be confirmed separately by a passport or ID card. So, you had to scan them for the materials
9.5. membership terminated
12.5 proposed change of gift from the company side (refused)
15.5 he company asked for confirmation from the home address. Had to send electricity or phone bill
18.5. company offered Amazon 20 € gift certificate (refused)
20.5 The order heard is processed and the gift is sent in a few days
26.5. asked where the gift goes
28.5. the company replied that the gift would come as soon as possible
16.6 latest message. They answered 19.6 that they cannot give an exact timetable, but the gift will come as soon as possible

Figure 4: Follow-up of giftcable.com shipment notification

The Swedish Consumer Agency and the European Consumer Agency carried out a quantitative research (Theorell, 2017) on consumer experiences in order of subscription payments in six different EU countries (Sweden, Finland, Holland, Belgium, Austria and Norway) from 27 February to 7 March 2017. The aim of the research was to find the phenomenon underlying the cases and to find out the extent of the cases. The purpose of the study was to find out how large this type of crime is.

The study (Theorell 2017) interviewed a total of 6112 consumers with an age distribution of 18 to 75 years. As a result of the research, it became clear how consumers in Sweden and especially in Finland, fall easily into these ”too good to be true” online deals. Of the surveyed consumers, Holland and Belgium had the highest number of consumers who fell for these online traps. From the point of view of age distribution, young people (18-29 years old) fall into such traps in Holland and Belgium. The 60- to 75-year-olds were again the most risky to fall for subscription traps in Sweden. Of all the respondents, the majority said they had somehow accessed the charger. In these notices, consumers informed the charger that they had not subscribed to any order or have directly attempted to cancel the order. Many, however, ended up being contented to pay the debited amount to the order company. About 10 percent of all respondents reported that they had contacted the bank or credit institution by making a complaint about the controversial charges. On average, consumers said they lost 115.70 euros for subscription companies over the last three years.

According to Theorell’s (2017) study, there are differences in the kind of attractive deals people are taking. Men are more interested in subscriptions that promote electronic gadgets or anti-virus software. Women are more inclined to subscriptions related to dieting, weight loss or beauty treatments. In terms of money, orders differ significantly between women and men. Men lose an average of 147 euros, while the average loss for women was 74 euros. This difference may be due to the fact that male-oriented products are more expensive than women’s products.

4. How do we fight against subscription traps?

Banks have increased the practice of removing the right to charge the subscription trap company if there is a significant amount of complaints from the said company. However, there are many problems with chargers (subscription trap companies) changing their own company name as well as their acquiring bank at regular intervals. It would be an impact if the situation were to be prevented already by the acquiring bank, i.e. subscription trap

companies would be screened more accurately before accepting merchants, and subscription trap companies along with incoming complaints would be constantly monitored. An important point is that social media companies and other misleading advertising platforms should be more responsible for their content. The problem should not be seen as a loss by just one particular individual, but the focus should be shifted on to how much profit these cybercriminals are making from thousands of individuals.

In the development of crime prevention, the police are searching for better tools for pre-trial investigations of individuals who are guilty of customer manipulation and misrepresentation. Respondents of this research poll want to develop consumer education and support effective international co-operation with authorities. Victims generally understand being scammed but they are afraid or able to resist claims. Banks should also be more aware of different scams and traps. In many countries, attention is often given to other cyber security problems, but not enough attention is given to subscription traps. Many of the responses emphasized the banks' responsibility to develop their banking systems so that they could better identify subscription traps and prevent the card from being used on scamming sites.

It would also be important to have a change of attitude: a subscription trap should not be seen as a problem for a single person. Continuous payments should be verified separately so that consumers can be aware of each transaction. The business is based precisely on the fact that the consumer is milked until he realizes that money is lost every month (Akerlof and Shiller, 2015). Misleading marketing costs should be the responsibility of the acquiring bank, thus liability and prevention is shifted to the initial stage. Reporting of suspicious activity should be rapid and should lead to actions in card schemes, to the corresponding authorities and the police. Information about crimes should be shared with policemen, especially in the area where the merchant is located. Stopping cash flow is the most effective way to stop subscription traps.

The aim of the case study is to find out about subscription traps and the different methods with which to fight them in the form of a questionnaire. The questionnaire was addressed to the researcher's professional network of contacts who have experience in subscription traps. The respondents were from the International Association of Financial Crimes Investigators, the European Cyber Crime and Fraud Investigators and the National Bureau of Investigation, colleagues in European banks and in Europol. Similar inquiries to consumers have been made elsewhere in Europe, but this survey was the first to target crime prevention professionals. The survey was held from 13 August to 13 September 2017 with 73 responders.

Many respondents reported that they had met subscription traps since the beginning of the year 2010. Banks and other financial institutions reported that the problem began to appear in 2013, while police reported that the problem was apparent in 2014. Many reported that subscribers still employ several hours a week, even though banks and financial institutions have taken a more direct approach to eliminating subscriber loopholes. The questionnaire revealed that most of the complaints related to subscription traps are so called unnecessary work and often time consuming, even though the background is ultimately the customer's reluctance and negligence. On the other hand, the versatile cheating and misleading advertising equation is challenging to explain to many consumers. Many representatives of the bank and the financial institution have said that since 2014 this is the largest single issue that they receive complaints about. The respondents estimate that 30-35 % of all complaints filed for processing are related to subscriptions.

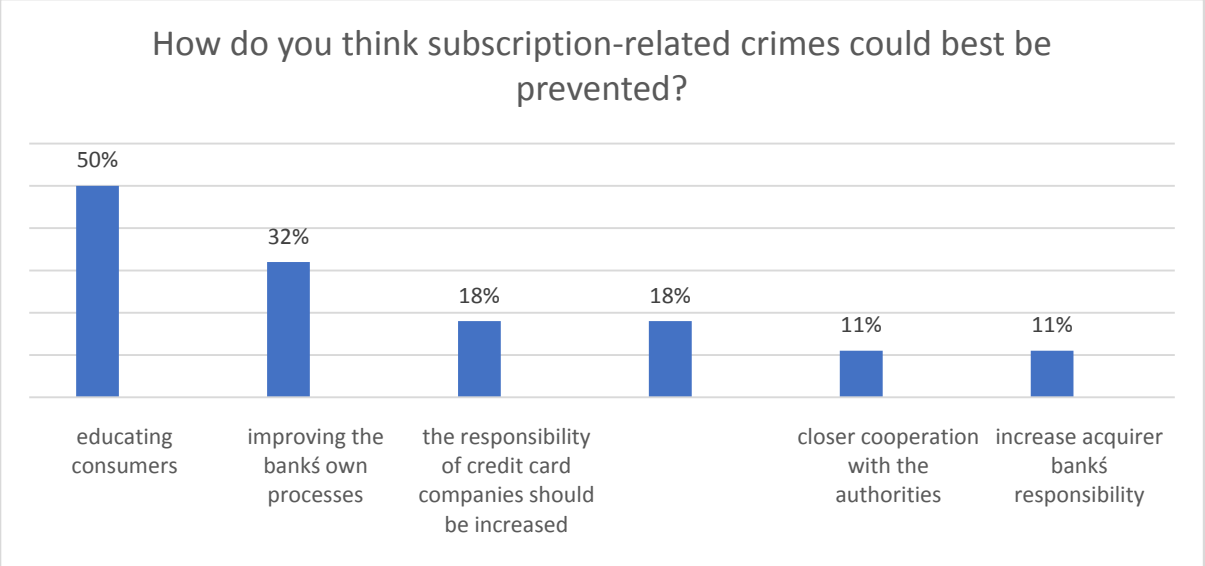

Figure 5: A survey was conducted to professionals who had experience in subscription traps and cybercrime.

Many of the responses highlighted the role of Denmark with regard to subscription traps. Of all the respondents 44% were concerned about the problem of subscription traps from Denmark for businesses and customers. There is also a problem that subscription companies frequently use and exchange acquiring banks all over the world, from Iceland to Mauritius. The survey showed that subscription trap crimes usually come from areas where legislation, information technology expertise and low capture support favor this kind of crime.

The survey respondents reported that 77% subscription traps complaints was not reported to the police. In addition to these figures, there are also consumers who do not report to the police and do not complain to their bank. The number of these consumers can only be guessed.

Detective sergeant Juuso Tschokkinen, a representative of the National Bureau of Investigation in Finland, comments on co-operation between this thesis and the National Bureau of Investigation in crime prevention of subscription traps:

"This study is a perfect example of a multidisciplinary approach to a complex security matter in the European Union. The study has been conducted by using multiple methods of data gathering from news services, internet search engines, police organizations and financial institutions in the EU. The study highlights that in the myriad of free movement of money and services in EU, there are actors who try to camouflage as legal enterprises but still cause substantial financial losses to the citizens of EU, falling sometimes between the cracks in the European Judicial framework and police practises. The study has helped the National Bureau of Investigation of Finland to communicate the phenomenon of new phishing methods to the wider European Law Enforcement community and is an excellent complementary piece of information to support the future work of the EMPACT (European Multidisciplinary Platform Against Criminal Threats) group of Law Enforcement experts regularly meeting at the European Law Enforcement Agency, Europol, in the framework of the EU Policy Cycle 2018-2021." (Tschokkinen, 2018.)

A subscription trap site is easy and quick to set up, and attractive ads are rapidly catching a large number of people. On the side of the

criminals the risk of losing money from creating a subscription trap is small. The problem is the growing number of social media, laxity, and the fact that in most countries subscription traps are not a criminal activity, but only a form of misleading of the consumer. There is no clear picture of whether your order is legitimate or illegal. Consumers and financial industry professionals do not recognize a clear criminal lawsuit that would result in a subscription trap company being illegal because the subscription traps do not always meet the criteria of fraud. It is not clear to which authority subscription traps belong. A major problem, especially from the financial world, has been a too loose screening of traders when making trade agreements. Card organizations, such as VISA and MasterCard, are also not in a position to prevent these types of cybercrime. Social media companies which provide targeted marketing should have responsibility in crime prevention associated with subscription traps. Still ongoing subscription campaigns are marketed aggressively by email, in Facebook and Instagram, and they can easily find the target markets in the digital world.

5. Results

Quality is measured by validity and reliability. According to Yin (2009), reliability and validity can be divided into four different parts: internal validity, external validity, reliability, and structural validity. In research, reliability refers to the repeatability of measurement results, which can be verified by various methods. A reliable research provides reproducible, non-random results. Valid or qualified research is the one where the set research method measures the right things, usually what is meant to be measured. The aforementioned concepts come from the world of quantitative research, in qualitative research they tend to be avoided. The starting point for all the studies is that they evaluate their reliability and qualifications.

The collection of research material was expected to be challenging because of the specific nature of the research topic. The material itself was not available, but majority of my data was collected by surveys and interviews. The respondents responded based on their own experiences, as they have studied subscription traps at work. Some of the respondents had experience with subscription traps, but not all were involved directly in crime prevention. The research material was based on the researcher's own subjective view of the role and significance of subscription traps to cybercrime as a whole.

In this research, reduction of the potential flaws in the data was done in two different ways. The widest possible range of respondents from Europe who have different experiences with subscription traps was sought. There was a fair number of respondents (73), which increased the reliability of the material. Another issue that raised the reliability of the research material was focusing on the questionnaire. Clarity of the questions, their form and their understandability were focused on. Initially sample questionnaires were made and given to a group of individuals (testers) who in turn gave their feedbacks and inputs about the questions. The questions then were formulated based on the inputs of these testers, such as process descriptions and factors involved in solving them. Only then were the questionnaires given to the respondents.

From the respondents, valuable insights into the phases of crime prevention was gained especially its challenges. Since little is known about subscription traps and there are only a few expert on the matter, it is important to find people who have been investigating these crimes and fighting against them. In the survey, the participants agreed that it is difficult to fight against this cross-border crime, especially when faced with anonymous enemies. Expert responses highlighted subjective but well-founded views on the challenges faced

by subscribers in crime prevention. The questionnaire revealed a disagreement over how to develop cooperation. The private sector emphasized more cooperation with the authorities and the exchange of information. The authorities, on the other hand, stressed that clearer penalties based on the law should be made in order for companies who make order subscriptions to abandon their activities. The private sector, more than the authorities, highlighted the need to fight against these subscription traps. According to the private sector, the police decide to terminate investigations involving foreign merchants and if the loss is only tens or at most hundreds of euros.

6. Conclusions

Special support and education should be focused on people whose digitalization skills are not at the par with the majority. Such target groups are, in particular, the weaker population and the population left out of digitalization. Enlightenment and information are often raised when talking about crime and the fight against crime. Who is responsible for educating consumers? The finance sector often thinks that education and information are part of the authorities whose resource problems generally hinder the large-scale consumer education.

Based on the questionnaire, it was clear that in some countries subscription traps are being managed or otherwise linked to these countries. IP addresses have also been studied, but they are also interchangeable and hence inaccurate to define which companies are being run. Based on the survey, there was a clear structure between countries, what products are being offered. The United States and North America are mainly used for weight loss products and cosmetics. Businesses from the United States are also much more difficult to investigate, as the charger name may be just a long set of random numbers.

The respondents were very unanimous about why subscription traps seem to be good business. A subscription company is relatively easy to set up on the internet, and ready-made applications and sites may be slightly modified for new businesses. Studies have shown sites that have only altered the colors on the site and the subscription product has been changed, also changed are the site's fonts, other layout, contacts. The authorities warn people at regular intervals on their own websites, and banks educate their customers about subscriptions and other dangers in online banking.

Criminals have come to realize how small the downside to the subscription traps is. The general discussion of whether penalties for subscription traps are covered by criminal law or the consumer law does not help improve crime prevention. For a large number of authorities and bank representatives, it is unclear what kind of crimes are involved and whether these are even criminal offenses. Many banks have also shifted subscription traps to be the customer's own responsibility and even blames the customer for not reading the terms.

The inefficiencies of the authorities also became one of the key issues in the survey. There was concern about the lack of tools for fighting crime against subscription traps. Legislators should be allowed to present this disadvantage in cyber security conferences around the world. The more publicity this problem gets, better awareness is directed to the legislators and the more likely the problem could be changed. To change this, cooperation with payment card associations is needed worldwide. Online criminals are anonymous and can do this kind of crime virtually anywhere in the world. It is hoped that authorities, banks and other financial institutions could more closely exchange information on new and emerging subscription traps. Communication should also be developed between banks and payment service providers to move information faster so as to respond to different types of suspicious activity.

References

Akerlof, G and Shiller, R. (2015). Phishing for Phools: The Economics of Manipulation and Deception, Princeton University Press, New Jersey.

Enforcement and European Consumer Centres, (2016). "Misleading free trials and subscription traps. [online document]. http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=25915&no=8

European Comission, (2017). The European Comission and Member States consumer authorities ask social media companies to comply with EU consumer rules. Retrieved on 8th December 2017 from http://europa.eu/rapid/press-release_IP-17-631_en.htm

Eurostat, (2017). Internet users who bought or ordered goods or services for private use over the internet in the previous 12 months by age groups. Retrieved on 15th November 2017 from http://ec.europa.eu/eurostat/statistics explained/index.php/File:Internet_users_who_bought_or_ordered_goods_or_services_for_private_use_over_the_internet_in_the_previous_12_months_by_age_groups,_EU-28,_2007-2016_(%25_of_internet_users).png

Heinonen, S. (2009). Sosiaalinen media, avauksia nettiyhteisöjen maailmaan ja vuorovaikutuksen uusiin muotoihin, TUTU-eJulkaisuja. [online document]. https://www.utu.fi/fi/yksikot/ffrc/julkaisut/e-tutu/Documents/eTutu_2009-1.pdf

Ilmarinen, V., Koskela, K. (2015). Digitalisaatio: yritysjohdon käsikirja, Talentum Media Oy, Helsinki.

Limnéll J., Majewski K., Salminen M. (2014). Kyberturvallisuus, Docendo Oy, Jyväskylä.

Nets Group, (2017), Nets Rolls Out Preventative Fraud Service to Protect Online Consumers Across the Nordics. Retrieved on November 22nd 2017 from https://www.nets.eu/Media-and-press/news/Pages/Nets-Rolls-Out-Preventative-Fraud-Service-to-Protect-Online-Consumers-Across-the-Nordics.aspx

Schmalleger, F. and Pittaro, M. (2008). "Crimes of the Internet", Pearson Education Ltd, New Jersey.

Theorell, C. (2017). Subscription traps in 6 EU countries 2017, Kantar Sifo. [online document]. https://forbrukereuropa.no/wp-content/uploads/2017/05/Summary_Subscription_traps_6_EU_countries_170424_Final_sifo_ECC.pdf

Tschokkinen, J. (2018). Multidisciplinary approach to a complex security matter in the European Union. [email].

Yin, R.K. (2009). Case Study Research Design and Methods, 4. edition, California.