**Skills building in Cybercrime**

**Case Study “Who am I?”**

**1. “Who am I?”**

1.1

Police service of Country A started to receive numerous complaints from citizens about strange cases of prize-winning games organized over social media networks by well known Brands from different commercial fields. Prize wins are different and tempting, ranging from market discount coupons up to flagship mobile phones or expensive lap-top computers. Games are organized on the social media networks in the way that on popular general communication channels Brands marketing teams are posting announcements of the games and prize wins inviting all people who are interested for taking part to join by clicking on the link which opens social media channel dedicated to the game. Hundreds and even thousands of people are attracted, and they are following the link and starting to participate in the game.

1.2

After some more or less usual questions which are presented as a short quiz on the Game channel, together with small participation fee payment, prize aspiring persons are getting information that he or she won the prize and that for the claim purpose personal data should be submitted. Instead of the phone number calling or e-mail sending to the Brand Prize Win Department, procedure is simplified in the way that only a photograph of the front and back of the personal ID card or passport of the prize winner, with him or her holding it, will be enough for the positive identification and claiming of the prize, as long as all personal identification details are clearly seen and that face of the person holding it and picture on the document are the same and clearly recognizable. Prizes are expensive, questions are easy, everybody wins, hundreds and thousands are happily sending photographs of them holding personal ID’s without a question.

1.3

However, something is not working properly. Happy prize winners although doing everything by the instructions are not being contacted by the Brand Prize Win Department nor they are getting prizes by the regular mail. Days are passing by and questions are rising. Some of the prize winners are starting to be worried about sharing their personal data and they start to check their bank and other financial accounts. However, it seems that everything is in order: not one cent has been stollen or unrightfully transferred. They start checking other services they are using, and all seems fine. Nothing is changed.

Situation starts to frustrate. Nothing is stollen or taken away and prizes are not delivered. What can be possibly wrong? To find that out, prize winners are starting to call the Brands headquarters which are all domestic based and to ask what is going on?

1.4

Customer Relations services of the Brands are taking the calls and they respond immediately to the prize winners: sorry, we are not organizing any prize-winning game now. Also, when such game is organized, it’s done in accordance with the respective Country A Law regulating gambling which guarantees protection of the personal data, what means that Brand would never ask for the public display of the personal ID.

Prize winners are starting to realize that they have been defrauded in some way, but it is not clear how and why. All banking and other accounts are un-changed and nothing is missing. So far, it seems that only personal data has been harvested and nothing more. Still, “prize winners” are angry because they have not got prizes and someone has their personal data, or even worse, photographs of their personal documents. They want answers and medias are starting to pay attention.

Police starts its preliminary investigation.

**2. Follow the data**

2.1

Police realizes that now thousands of the citizens of Country A have taken part in some version of the prize-winning game. Brands are different, domestic, or foreign, but all are based in the Country A in some way. Bank and other financial or property accounts are checked and indeed nothing is missing. Social-Media Networks are both domestic and international hosted. It seems that there is no rule about it, except that they must be popular. Request has been dispatched to the Networks with certain questions and action demands. Results are starting to be received by the police and first clues are emerging. Internet Service Providers are now included in the investigation. Results of certain police actions are giving results. First suspects are identified.

2.2

Certain procedural measures and orders by the Prosecution and Court are acquired and in motion. Evidence in regular or electronic form are starting to be acquired. Reasonable doubt that crime has been perpetrated is established. Evidence and interrogations are showing that group of the people who are not necessarily connected is posting information about prize winning games on either original or false social media channels of the Brands. Access to the original channels is made possible by unlawful acquirement of the logging credentials. If the channels are false, copies of the original Brand labelling are used. Fraudulently acquired personal data is in fact a commodity. It is sold to persons on the Dark Market hosted in Country A who are paying between 15 and 50 Euros per photograph, depending on the quality. Money is transferred sometimes on bank accounts, sometimes in cryptocurrency.

**3. Follow the money**

3.1

Additional information is acquired. Next suspects in the chain are identified and additional measures and actions are undertaken under Prosecution or Court orders. Evidentiary actions and measures are giving results. Electronic evidence and interrogation are showing that personal data information bought on Dark Market is actually used for opening of the payment accounts with on-line payment company residing in the Country B, which endorse voluntary cooperation. Payment accounts are opened on the name of the person whos’ ID card and photograph has been used. Photograph is one of the conditions for opening of the account. Further investigation is showing that newly opened accounts are within 24/48 hours receiving deposits of 1000 EUR each payed in cryptocurrency. Since hundreds or thousands of accounts are used, it is starting to be clear that significant money is in the motion.

3.2

Further investigation shows that on-line payment accounts in Country B are having connection with Country C accounts with on-line betting company, which does not endorse voluntary cooperation. It seems that the same names and same personal ID’s are used for opening of the on-line betting accounts in the Country C. Additional investigation actions are showing that very soon after the initial down-payment of the 1000 EUR to account in Country B is transferred to the betting account in Country C. Net cash flow is full, meaning that nothing stays in the Country B and all the money is transferred to the Country C.

Next set of the investigation actions takes place and results are showing that money is indeed payed to the accounts in Country C but not for long. Within 24 to 48 hours it is again transferred back to the accounts from which initial payment was done. After the transfer, accounts in on-line betting company are closed and deleted permanently.

**4. Follow the leader**

4.1

Investigation now turns back to the Country B and accounts with on-line payment company. All of the accounts from which initial payments were done and which were empty now are having again 1000 EUR on them under the names of the ”prize winning” people from Country A.

Further evidence analysis shows that within short period of time transactions are made between on-line payment accounts and, this time, banking accounts of the individuals in the Country A. Transfer is full and all 1000 Euros are transferred. After the transfer has been made accounts are closed and deleted on Country B platform. Country A Police Force continues investigation. Additional information and evidence are gathered, and they show that there is certain number of individuals in Country A who are receiving payments from Country B. It seems that some level of the coordination exists amongst them since on the same day they are either visiting banks or using ATM’s for money withdrawal of the almost identical sums.

4.2

What seems interesting is that on some accounts not all the money has been withdrawn and that some 5 to 10% is staying. However, communication between individuals is continued in some way since this kind of action ensues until either all the money is withdrawn or certain percentage stays.

Police continues with the investigation. Additional Prosecution and Court orders are acquired, and Action Day is set. During field action number of individuals are arrested and electronic and regular evidence are obtained. It seems that not much of the money has been seized. Interrogation records are showing that suspects are using social media and VOIP services to contact a person from Country E. Some of the messages are showing that suspects are expecting to hand over cash money to that person either when it arrives to Country A or when they travel to Country E which is neighbouring one.