Identity theft essay

Technology, Internet

\n[toc title="Table of Contents"]\n

\n \t

\n[/toc]\n \n

Identity theft form of cyber-crime was identified by Golladay and Kristy (6) to have started in the early 21st century when it became indispensable for individuals to use personal bits of information in making online payments or social activities. For identity theft to occur, the fraudster has to collect personal information of the target victim that can be maliciously used to impersonate the victim and carry out business on behalf of the victim. The success of the identity theft depends on the victim letting down their guard by being less vigil and strict on the need to have tight security measures for all online transactions. For example, through the internet based internet platforms, individuals do not have to present physical evidence or presence to gain access to funds or products. In the modern day business world, the use of a physical signature or need to see the signatory has been replaced by the use of codes. When a criminal has access to a victim’s details such as social security number, ID names, address and phone number, they can use the details to commit fraud in the name of the individual (Jennings, 44).

Identity theft examples

A good example to illustrate what the identity theft entails is the numerous cases of impersonation in the social media platform of internet. A fraudster

can collect images of the target victim, create a fake social media account under the name of the target victim. Then the fraudsters send a friend request or invitations to the victim’s social media accounts. After befriending the victim's friends, the fraudster; s confidences the victim; s friend that they are in an emergency and urgent need of funds. Without confirming the emergency, the victim; s friend sends funds to a newly provided funds account of the fraudster which bears the name of the victim.

Identity theft is often accomplished under the scenario that the malicious person gathers enough personal information about the target victim which then can be used to act maliciously on behalf of the victim. To collect the personal information, the fraudsters can use several methods such as physically stealing the information or through the virtual platform of hacking (Insurance Information Institute). The idea is to collect enough information that can convince a third party to release funds or oblige to the commands of the fraudster. The result of identity theft, in most cases, is always the same, regardless of how the fraudster obtains the personal information. The outcome is in the scope of the fraudster authorizing or acting on behalf of the victim for their personal benefit, either monetary or revenge.

Identity theft cases

Jennings (42) identified that identity theft fraudsters normally targeted their victims by four main demographics of age, social, economic class, computer users with poor passwords and people using shared computers. Research indicates that the age bracket of 18-24 years is likely to be targeted. The above is due to the statistics that depict the age bracket as to be highly

active in online shopping. Additionally, the age bracket does not have much experience on how to go about protecting their personal information. The next group is the economic class earning over $75, 000. The criminals target wealthy victims because they are likely to have more funds in their credit cards accounts. The wealthy groups also conduct multiple shopping activities using their cards, and it is thus easier for fraudsters to convince third parties to release funds. The group of people using public computers is appropriate for the fraudsters because the fraudsters get an easier platform to dig for personal information. Victims who use the cyber as a platform for accessing their credit cards account are at a greater risk (Insurance Information Institute). The criminals first deposits virus programs that can harvest passwords for every user who uses the public computer. People with weak passwords presents an easy target for the criminals because easy passwords can be cracked using complicated programs. Fraudsters acknowledge that the easier the password, the easier it is for them to crack.

Identity theft over the internet platform is a common and trending practice and accounts only for the large margin of internet crimes, almost half of cyber-crimes. However, literature such as Jennings (23) argued that the statistics may be higher because not many people report or even notice that their identity has been stolen and used fraudulently. A report released by Javelin Strategy ; Research, in 2016, found that a sum of $15 billion had been stolen from around 13. 3 million U. S. consumers in the year 2015 (Insurance Information Institute). Javelin Strategy ; Research, in 2015, had reported that in 2014 a sum of $16 billion had been stolen from 12. 7 U. S. citizens (Insurance Information Institute). The above illustrates that there are

increasing scenarios of victims being defrauded by identity thieves. The impact of the increased identity theft is that it lowers the benefits of online shopping as more and more people become hesitant to conduct online business for fear of being defrauded.

Works Cited

Golladay, Katelyn, and Kristy Holtfreter. " The Consequences of Identity Theft Victimization: An Examination of Emotional and Physical Health Outcomes." Victims ; Offenders, 2016, pp. 1-20.

Insurance Information Institute. " Identity Theft And Cybercrime." Insurance Information Institute, www. iii. org/fact-statistic/identity-theft-and-cybercrime. Accessed 10 Feb. 2017.

Jennings, Judy, and Kirk Fagerland. Help! They Stole My Name!: The Impact of Identity Theft.