Student’s name

Instructor’s name

Course

Date

Identity Theft

Rapid technological advancement and the integration of the Internet in all spheres of human activity has allowed individuals and businesses to utilize more information and data for their needs and business operations. The significant digitization of information and processes eases the use of banking services, purchasing platforms, social media, and web applications. While the use of Internet technologies and personal devices makes people's lives convenient, the intensive use of web technology increases risks of cybercrimes, like identity theft. Even though modern companies ensure people that security measures are high and advanced, the loss of documents, data breaches, and sensitive information leaks have become the most concerning issues in the 21st century.

Identity Theft and Cybercrimes

Identity theft is a specific type of cybercrime when criminals gain access to a victim's private information to use for other crimes ("Identity Theft"). Private information may contain the victim's real name, address, identification number, social security number, medical coverage ID, passwords, credit card data, and workplace sensitive information. This stolen data can be used for financial crimes, blackmail, information sales, or for another instance of identity theft

when criminals use previous victims' data to mask their presence and mislead enforcement bodies ("Facts + Statistics: Identity Theft and Cybercrime"). Significant issues and damages are caused by those who work in the public segment, have access to business entities' sensitive information, or people who are involved in international relations, trade, or politics ("Identity Theft"). Nonetheless, ordinary people also have value for cybercriminals, as social media profiles, purchase history, and personal information can be used to conduct other crimes, like DDoS attacks, hacking, spamming, and security breach exploitation.

Moreover, identity theft uses social media data for sales as marketing companies, retailers, and large enterprises prefer black markets to acquire this information and employ it for marketing, advertising, and sales purposes. Most often, victims of such cybercrime begin to receive spam, advertising emails, or suddenly uncover that they are subscribers of suspicious social groups, forums, platforms, or companies' client lists ("Facts + Statistics: Identity Theft and Cybercrime"). In this case, identity theft possesses a prominent threat for private information security and may lead to the loss not only of funds or social media profiles but also more severe consequences, like driving licenses, medical coverage, and ID information replacement or duplication.

Consequences of Identity Theft

The consequences of identity theft vary from fraud and light issues to money loss and document theft. According to the Information Insurance Institute (III), in 2018, people reported 1.4 million fraud-related cybercrimes, where 25% led to money loss ("Facts + Statistics: Identity Theft and Cybercrime"). The Institute reported that consumers lost more than $1 billion due to

identity theft. The most common identity theft cares are scams, viruses which cipher data, and demanding a sum for the decoding ("Facts + Statistics: Identity Theft and Cybercrime"). People who become victims of cybercrime pay $365 on average; however, the general loss of money is near $490 million ("Facts + Statistics: Identity Theft and Cybercrime"). Furthermore, the consequences only get worse in scale with time.

Furthermore, the top identity theft is related to credit card history and data theft, which results in new account creation, loans, and mortgages. Victims of this cybercrime have limited resources and opportunities to state that they do not open or sign up for additional banking services; however, the only way to recover lost data and cancel any contracts is the court and to complain to enforcement bodies with the request for an investigation ("Recovering from Identity Theft"). Also, tax fraud is a new trend among identity theives, as they use victims' ID numbers and taxpayer information to omit taxes or launder money. Near to 40,000 people complain that they have become victims of such a crime and should pay more than $488 million for non-existing business operations and profits ("Facts + Statistics: Identity Theft and Cybercrime"). As a result, identity theft causes financial losses for both individuals and business entities, causing a loss of reputation, court hearings, and financial devastation.

While financial crimes, with the help of identity theft, has become a common phenomenon, some people report that they also lost their medical coverage, social security numbers, and driving licenses. These complaints represent 10% of all identity theft reports; however, most of the victims were accused of severe crimes, as previously it was believed that they conducted these violations were due to discovered duplicates of their documents ("Identity Theft"). While there are some unified enforcement programs to protect identity theft victims

from misleading accusations, the issue with faultily detained people due to identity theft is increasing each year.

Recovery Plan and Prevention

The identity theft recovery plan is a set of recommendations developed by the Federal Trade Commission, Credit Bureaus, and Enforcement Bodies. The document encompasses several steps for general information security, sensitive data safety, and specific actions related to severe or unique types of identity theft ("Identity Theft: A Recovery Plan" 1). The recovery plan aims to protect citizens from fraud and educate them about secure methods of Internet use, applications and software purchases, online activities and information exchanges, and personal data storage.

The document indicates that due to the increased number of complaints and cybercrimes, citizens should be aware of where and who may use their personal information. The recovery plan suggests that people should frequently ask for reports and checks to ensure that their sensitive data is not used by unauthorized parties ("Identity Theft: A Recovery Plan" 2-3). In this case, the recovery plan offers several steps to recover stolen data or protect sensitive information from identity theft.

Foremost, the recovery plan targets those who are victims of identity theft so that the first recommended step is to call companies where the fraud could take place and ask to freeze all accounts or services due to the identity theft. Moreover, the recovery plan suggests asking for an activity report to identify whether personal information was used or not ("Recovering from Identity Theft"). Then, people should contact the bank and ask to freeze credit cards and

accounts to prevent financial loss. Simultaneously, the recovery plan highlights the urgency of password, login, and pin changes to avoid more information leaks.

After proceeding with these steps, the victim of identity theft should personally go to the police and write a detailed complaint about when, how, and where the fraud occured. In this case, the chances to protect and recover data are high; however, it almost impossible to identify the cybercriminal or discover his or her motives ("Identity Theft"). Nonetheless, the recovery plan indicates that after the information change and the replacement of old data, the repetition of the fraud is low. Still, people are asked to pay attention to where and whom they reveal their private information to.

Conclusion

Identity theft is a new type of cybercrime which has becomes popular due to the increase in Internet and web application use. The loss of personal data involves severe consequences for victims, as criminals may get access to financial and social data, which are essential for public services, tax payments, and banking services. In case such fraud happens, victims should follow a recovery plan to regain access and control over their sensitive data. If the identity theft victim does not follow the procedure, a complete loss of data may occur, leading to financial devastation.

Works Cited

"Identity Theft: A Recovery Plan". *Federal Trade Commission*, 2016, https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf. Accessed 8 July 2019.

"Facts + Statistics: Identity Theft and Cybercrime". *Iii.Org*, 2019, https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

"Identity Theft". *Usa.Gov*, 2019, https://www.usa.gov/identity-theft.

"Recovering from Identity Theft". *Consumer.Gov*, 2019, https://www.consumer.gov/articles/1016-recovering-identity-theft.