Expert Report on Cyber-Identity Theft in Mexico

Muhammad Q

PDFCYL_PCOM7E November 2022

Dr Stelios Sotiriadis

Feburary 20th, 2023

Introduction:

Cyber-identity theft is one of the most pervasive and destructive types of crime in the digital age. It refers to the fraudulent use of someone's personal information gathered often online without their consent (Badiya et al., 2020). As digital technologies are used more often, it has become simpler for thieves to get personal information and utilize it for unlawful purposes. As a result, there is an increasing demand for strong security measures to secure personal data. Mexico is also a part of this pattern. Cyber-identity theft has increased recently in the nation, hurting people, businesses, and the economy as a whole. As a result, there is an increasing need to comprehend the nature of the issue and create solutions.

This report aims to provide a comprehensive overview of cyber-identity theft in Mexico, including its manifestation, rights, and ethical considerations, the effectiveness of national law, the availability and limitations of investigative tools, and the implications and perceptions surrounding victims, harm, perpetrators, and social perception (Bonina & Eaton, 2020). The report is based on extensive independent research, using published papers and journals as sources. The objective is to provide policy advice to the government of Mexico on how to address the problem of cyber-identity theft and to inform the public about the dangers and implications of this crime.

The research begins by examining the manifestations of cyber-identity theft in Mexico and its global implications. The legal and moral ramifications of prosecuting these offenses are also taken into account in this section. The efficiency of the national law in combating cyber-identity theft is then assessed, with an emphasis on its criminality, capture, and prevention. This section also evaluates the accessibility and constraints of investigation tools, notably digital forensic evidence (Choi et al., 2021). The paper then critically evaluates the issues by examining the ramifications and attitudes surrounding victims, harm, perpetrators, and society's perception. This research seeks to offer a thorough overview of cyber-identity theft in Mexico and contribute to creating efficient countermeasures.

Manifestation of Cyber-Identity Theft in Mexico:

Cyber-identity theft is an issue that is seriously affecting people, businesses, and society at large in Mexico. The most common form the problem has taken is the wrongful use of private data for gainful commercial activity. It might entail misusing credit card details, bank account information, and other delicate personal information.

As in many other nations, phishing scams are now a typical method of cyber-identity theft in Mexico. In these scams, victims get an email or message that looks to be from a reputable organization, like a bank, a government department, or an online merchant. Sensitive data, such as login credentials, credit card details, or personal identification numbers, are frequently requested in the message. Con artists use these details to conduct unlawful business, steal money, or break into secure systems. For instance, a phishing scam in Mexico is an email purporting to be from a bank requesting that the receiver click on a link and enter their login details to confirm their account. The link directs the victim to a bogus website that impersonates the bank's official website (Enoch et al., 2013). Once the person supplies their login credentials, the con artist can utilize them to gain access to their bank account and withdraw money.

A subset of malicious software known as malware targets or degrades computer systems. Hackers use this software to access private information and steal personal data. Those ransomware attacks that encrypt the victim's data and demand payment in exchange for the decryption key are examples of ransomware attacks in Mexico. In another occurrence, the malware was employed to record the credit card details of internet shoppers as they completed their purchases. Then, this information was either used in unlawful transactions or sold on the black market. Spyware is yet another infection utilized in online identity theft (Holt et al., 2022). Without the users' awareness, this software is made to watch over their behavior. Spyware has been employed in Mexico to steal bank account numbers, passwords, and sensitive financial information. The data was after that used to carry out illegal operations or to sell the data on the black market.

Social engineering strategies take advantage of victims' emotions and sense of trust to deceive them, making them a particularly dangerous form of cyber-identity theft in Mexico. Con artists frequently use psychological tricks like urgency, anxiety, or flattery to get victims to give private information. These strategies can be very successful, especially if the con artist can instill a sense of urgency or emergency, such as asserting that a prize would be forfeited if the information is not provided right away or an account has been compromised. The creation of bogus government websites is just one illustration of a social engineering attack in Mexico (Kobek, 2017). Scammers frequently produce counterfeit government portals or websites that resemble real ones, such as those of the Mexican Ministry of Finance or the Mexican Social Security Institute. Once users have provided important information, such as their social security number, bank account information, or login credentials, these bogus websites are utilized to deceive them. The harm produced by the attack is sometimes further exacerbated by the scammers' requests for money or fees to be paid via the website.

Additionally, data breaches at organizations, including public and commercial sector entities, may result in cyber-identity theft. Large amounts of personal data may be stolen due to these breaches, which may be used illegally.

Rights and Ethics Considerations:

In Mexico, cyber-identity theft is a rising problem threatening private rights and prompting moral and legal questions. People are more susceptible to cybercrime due to collecting and storing sensitive information on digital devices, including bank account information, personal identification numbers, and other private data. The Federal Law on the Protection of Personal Data Held by Private Parties and the Federal Law for the Prevention and Identification of Money Laundering are two pieces of legislation Mexico has developed to protect privacy rights in response to these worries.

However, despite these efforts, some experts argue that more than these laws are needed to protect individuals from cyber-identity theft. For example, the Federal Law on the Protection of Personal Data Held by Private Parties only applies to private entities and not the government, which leaves a significant gap in privacy protection. In addition, the penalties for violating privacy rights are often insufficient to deter potential cyber-criminals (Sunde & Dror, 2019). One high-profile case in Mexico highlighting the need for stronger privacy protection is the data breach of Mexico's National Electoral Institute (INE) in 2018. The breach resulted in the personal data of over 93 million Mexican citizens, including names, addresses, and voter ID numbers, being leaked online. It was a clear violation of privacy rights, and such a large amount of publicly available sensitive information demonstrated the need for stronger privacy laws in Mexico.

Effectiveness of National Law in Dealing with Cyber-Identity Theft:

Mexico has a comprehensive legal framework to combat cyber-identity theft. The Mexican Federal Criminal Code contains provisions that criminalize computer-related crimes such as hacking, data theft, and identity theft. The National Commission for the Protection and Defense of Personal Data oversees Mexico's privacy and data protection laws (Summers, 2012). There are also various federal and state-level regulations to protect individuals from cyber-identity theft, such as the Mexican Federal Law for the Protection of Personal Data Held by Third Parties.

Experts are worried about how well current laws address cyber-identity theft despite these legal safeguards. According to a recognized research institute, cybercrime has been rising in Mexico despite regulations designed to deter it. Additionally, the study discovered that many cybercrime occurrences in Mexico go undetected, making it challenging to determine the full scope of the issue (Rodriguez & Velásquez, 2021). The inadequate application of present regulations is one of Mexico's biggest obstacles to combating cyber-identity theft. It is difficult for Mexican law enforcement to pursue those involved in cyber-identity theft because many of them are based outside of Mexico. Additionally, the bureaucratic and slow nature of the Mexican judicial system is widely criticized, which leads to protracted court cases that may take years to be resolved.

More legislation is necessary to address the growing issue of cyber-identity theft in Mexico in light of these difficulties. It might involve toughening up the penalties for cyber-identity theft, expanding the effectiveness and timeliness of the court system, and strengthening law enforcement's capacity to look into and prosecute cybercrime (Roberts, 2009). More public education is also required regarding the risks of cyber-identity theft and the steps that may be taken to prevent it. Although Mexico has a strong legal system to combat cyber-identity theft, its efficiency is a cause for concern. The threat of cybercrime in Mexico is rising, emphasizing the need for more legislation, enforcement measures, and public education on the subject. A comprehensive strategy combining the cooperation of governmental organizations, law enforcement, and the general public will be needed to address cyber-identity theft.

Investigative Tools for Cyber-Identity Theft:

Investigative tools are crucial for preventing and handling cyber-identity theft scenarios. They support law enforcement in intelligence collecting, suspect tracking, and suspect prosecution. To combat cyber-identity theft, Mexico has a variety of investigation tactics at its disposal, but it is important to consider their accessibility and limitations.

Digital forensics is one of the most often employed investigation techniques. It entails looking through electronic devices like computers and cell phones for signs of illicit activity. One can utilize digital forensics to retrieve destroyed files, spot hacking efforts, and find suspects (Navarro, 2016). It can take much time and requires specialist knowledge, which might prevent law enforcement organizations from using it. Network analysis, which analyses online traffic to find patterns of illegal activity, is another investigative tool. This tool can assist law enforcement in finding suspects and determining the scope of the cybercrime issue. However, network analysis calls for extensive data access, which can be challenging to acquire.

Analyzing social media is a helpful investigative technique for cyber-identity theft. Social networking sites like Facebook and Twitter can provide much evidence on suspects, such as their internet habits and private information. Law enforcement can use these details to develop a case against suspects and find additional people who might be connected to the crime. However, privacy issues can make social media analysis less useful as a research tool.

Last, blockchain analysis can be used to look into cyber-identity theft. Blockchain data, including cryptocurrency transactions, must be analyzed to find proof of criminal activity. Law enforcement agencies can trace suspects and retrieve stolen money using blockchain analysis. However, blockchain analysis is still in its infancy, and it still needs to be clarified how useful it will be as a research tool. While various investigative techniques are available in Mexico to combat cyber-identity theft, their efficacy and limits must be considered (Marques & Serra, 2016). Various instruments are required for law enforcement organizations to effectively combat the expanding issue of cyber-identity theft and hold offenders accountable. To keep up with the growing threat of cybercrime, it is also essential to develop new and creative investigation methods.

Victims, Harm, Perpetrators, and Social Perception:

Cyber-identity theft is a crime that negatively affects victims, property, offenders, and the public's perception. This act's victims could suffer additional damages, including financial loss, harm to their reputation, and invasion of privacy. For instance, a victim of online identity theft may experience bank account draining or a decline in credit rating. It might have a long-lasting impact on their financial stability and ability to get loans in the future (Kobek, 2017). Cyber-identity thieves might commit fraud, identity theft, or the sale of personal information using the information they have gained, among other crimes. These criminals typically carry out crimes to make money. These individuals might be home-based hackers or small-time criminal gangs.

Different people view cyber-identity theft differently, with some seeing it as a crime with no victims and others seeing the serious harm it does. A rising number of people are becoming aware of the problem and the significance of taking precautions to protect themselves, including using strong passwords and exercising caution when disclosing personal information online. Despite the threat of cyber-identity theft being more widely acknowledged, some people still do not grasp it (Holt et al., 2022). It could lead to a lack of sympathy for the victims and an unwillingness to take precautions to save oneself from the crime. Law enforcement agencies, governments, and organizations must collaborate to combat cyber-identity theft and assist victims. It entails enhancing public awareness of the problem, offering victims tools for reporting crimes, and boosting law enforcement's efficiency in catching and convicting offenders. By taking these actions, we may lessen the damage done by cyber-identity theft and raise awareness of the significance of online data security.

Conclusion:

The expanding issue of cyber-identity theft has created various challenges for Mexico's criminal justice system and law enforcement. It has been questioned if the national law reduces crime. Therefore, new legislation is required to address the issue. Even though they are infrequently used, access to investigative tools is essential for finding and apprehending perpetrators (Badiya et al., 2020). Despite this, many victims of cyber-identity theft still struggle to recover the information taken from them and receive compensation for their losses. It is important to consider the social aspect of online identity theft. Because of the stigma attached to them, it could be difficult for victims of cybercrime to ask for assistance and report the crime. Increasing public trust in law enforcement's ability to protect citizens from cybercrime and bring perpetrators accountable is another challenge.

Cyber-identity theft has become a major issue in Mexico, with numerous forms of manifestation, including phishing scams, malware and malicious software, and social engineering tactics. The use of digital devices to store sensitive information has made individuals vulnerable to cybercrime, and current privacy laws may not be sufficient to protect individuals from cyber-identity theft (Bonina & Eaton, 2020). Despite national laws aimed at criminalizing, apprehending, and preventing cyber-identity theft, their effectiveness has been criticized, and there is a need for more effective enforcement and new legislation. Regarding investigative tools, several resources are available to authorities and individuals in Mexico, including data forensics and investigations, technical surveillance, and online monitoring. However, the effectiveness of these tools depends on the skill and resources of the individual or agency utilizing them.

Cyber-identity theft can seriously affect victims, leaving them with mental distress, financial loss, and reputational damage. The perpetrators of cyber-identity theft can be either people working alone or organized criminal groups, and their motives might range from financial gain to malicious purposes (Sunde & Dror, 2019). Regarding social perception, cyber-identity theft is a problem well-acknowledged in Mexico, where people are becoming more aware of the risks and potential repercussions of such crimes. More outreach and education campaigns are required to increase public awareness of the problem and motivate people to take precautions against cybercrime.

References

Badiya, A., Kapoor, N., & Menezes, R. (2020). "Chain of custody (chain of evidence)." StatPearls Publishing LLC.

Bonina, C., & Eaton, B. (2020). Cultivating open government data platform ecosystems through governance: Lessons from Buenos Aires, Mexico City, and Montevideo. *Government Information Quarterly, 37*(3), 101479.

Choi, J., Kruis, N.E., & Choo, K.S. (2021). "The impact of routine activities on fear of identity theft victimization." Journal of Contemporary Criminal Justice, 37(3), pp.406-426.

Enoch, Y. S., John, A. K., & Olumuyiwa, A. E. (2013). Mitigating Cyber Identity Fraud using Advanced Multi Anti-Phishing Technique. *International Journal of Advanced Computer Science and Applications*, *4*(3), 156-164.

Holt, T., Bossler, A., & Seigfried-Spellar, K. (2022). "Cybercrime and digital forensics: An overview." New York: Routledge.

Kobek, L. P. (2017). The State of Cybersecurity in Mexico: An Overview. *Wilson Centre's Mexico Institute, Jan*.

Marques-Arpa, T., & Serra-Ruiz, J. (2016). "The process of obtaining and sharing digital evidence." International Journal of Chaotic Computing (IJCC), 4: 79-86.

Navarro, C. (2016). Mexico Among the Top Countries in the World Facing Identity Theft.

Roberts, L.D. (2009). "Technoethics and cyber identity theft." Handbook of research on techno ethics, pp. 542-557. IGI Global.

Rodriguez-Hernandez, S. M., & Velásquez, N. (2021). Mexico and Cybersecurity: Policies, challenges, and concerns. In *Routledge Companion to Global Cyber-Security Strategy* (pp. 484-493). Routledge.

Summers, C. (2012). "An introduction to crime scene forensics."

Sunde, N. & Dror, I. (2019). "A review of cognitive and human factors in digital forensics." Digital Investigation, 29: 101-108.