Commission on Crime Prevention and Criminal Justice

CIMUN

Topic 1: Taking Measures to Prevent Internet Fraud

Anwita Karanth and Beatriz Silva

Introduction

As our emerging society continues to develop technologically, it is crucial that we are properly equipped to tackle the issues that inevitably arise from our own innovations. One of said matters is internet fraud- A cybercrime which utilises technology to harass and steal from other individuals for personal profit. Though this is becoming increasingly more common, it is still a severe infringement of act 12 in the Declaration of Human Rights, which entitles every human being to a right to their own privacy, as well as protects them from any sort of non-consensual breaching of their personal information. Thus, it is crucial that an appropriate proposal is put forward in regards to the issue, since without it, it's detriments will only worsen. In the United States alone, internet fraud increased by 25% in the first quarter of 2021, with the most targeted industry being that of finance[1]. In the previous year, over $3.3 billion dollars were stolen as a result of internet fraud[2].

The technology used by cybercriminals continuously develops to hinder police interference, such as through the use of a VPN or an untraceable device. These adaptations make it difficult to trace the culprit and thus the crime cannot be handled efficiently and the process is more rigorous and timely for those involved. As a result, it is urgent that measures are created to prevent the circumstance from being carried out, rather than to help tackle the issue once it has occurred, since cybercriminals have proved time and again that they can conceal themselves despite the protocols followed.

Key Terms

Internet fraud- the use of Internet services or software with Internet access to defraud victims or to otherwise take advantage of them[3]

Cybercrime- a crime that involves a computer and a network[4]

Cybercriminals- individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit[5]

[1] https://www.cnbc.com/2021/06/03/why-online-fraud-attempts-are-up-25percent-in-the-us.html
[2] https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime
[3]https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud#:~:text=Internet%20fraud%20is%20the%20use,the%20Internet%20through%20various%20methods.
[4]https://en.wikipedia.org/wiki/Cybercrime#:~:text=Cybercrime%20is%20a%20crime%20that,someone's%20security%20and%20financial%20health.
[5] https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals

Identity theft- when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes[6]

Universal Declaration of Human Rights- an international document adopted by the United Nations General Assembly that enshrines the rights and freedoms of all human beings[7]

Email scams- intentional deception for either personal gain or to damage another individual by means of email. Almost as soon as email became widely used, it began to be used as a means to defraud people. Email fraud can take the form of a "con game", or scam[8]

Lottery fraud- any act committed to defraud a lottery game. A perpetrator attempts to win a jackpot prize through fraudulent means. The aim is to defraud the organisation running the lottery of money, or in the case of a stolen lottery ticket, to defraud an individual of their legitimately won prize[9]

Tax fraud- when an individual or business entity willfully and intentionally falsifies information on a tax return to limit the amount of tax liability[10]

Background Information

Internet fraud in itself is not a new concept, in fact it can be first traced back to the early 1990's with the start of e-commerce in the United States[11]. During this time, stolen credit cards would be used in the name of wealthy and well-known individuals to make large transactions and purchases. As the online commercial industry was only just beginning, employees and business owners had no systems in place to check the legitimacy of these transactions, and thus the fraudsters got away with doing so. Soon after, another form of internet fraud was created- the use of credit card generators. Apps were created and available to the public in which real credit card numbers were generated, and which fraudsters used to make purchases. At this time, it was also common to consistently fraud one merchant or business, rather than frauding business after another. At the time, this diminished their chances of getting caught.

However, despite their advancements in frauding techniques, the way in which they gathered credit cards to fraud remained mostly the same; Dumpster diving, nail theft, pickpocketing, and

[6] https://en.wikipedia.org/wiki/Identity_theft
[7] https://en.wikipedia.org/wiki/Universal_Declaration_of_Human_Rights
[8] https://en.wikipedia.org/wiki/Email_fraud#:~:text=Email%20fraud%20(or%20email%20scam,con%20game%22%2C%20or%20scam.
[9] https://en.wikipedia.org/wiki/Lottery_fraud#:~:text=Lottery%20fraud%20is%20any%20act,of%20their%20legitimately%20won%20prize.
[10] https://www.investopedia.com/terms/t/tax-fraud.asp#:~:text=Tax%20fraud%20occurs%20when%20an,paying%20the%20entire%20tax%20obligation.
[11] http://www.fraudpractice.com/fl-fraudhist.html

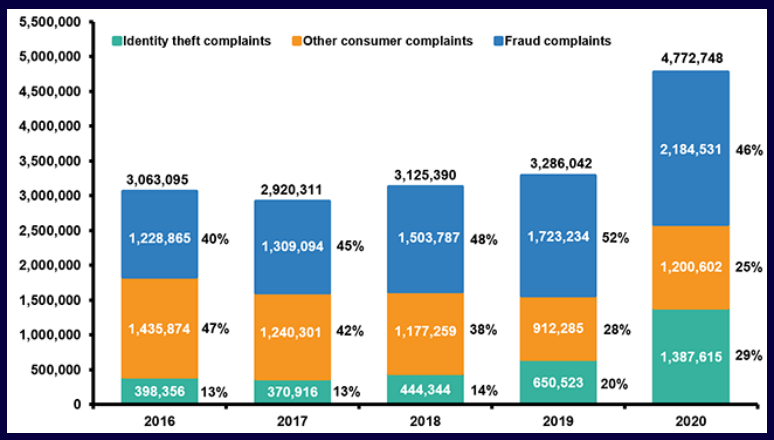
ect. That was, up until the internet continued to develop and e-commerce dominated the market. Fraudsters then began to use the internet as a way to steal credit card information, test them, and fraud them. They hijacked orders, hacked merchant sites, and even contacted the businesses to change the delivery address of several shipments so that they could take them.

By the early 2000's internet fraud began being recognized as an upcoming issue, and thus security measures tightened. In response to this cybercriminals initiated a new method of committing internet fraud- Using 'dummy websites'. Fraudsters would create and run a false merchandising chain, in which people would purchase their false products. The fraudsters would then keep the full profit from the transaction and would also have access to the credit card details of the victims, thus allowing them to use their information for other forms of fraud.

Following this, emerged the first occasions of identity theft- now one of the most common type of internet fraud. One of the most well-known instances of this was the mass identity theft of Military ID's, which allowed fraudsters to take advantage of military discounts and thus take revenue from merchandisers.

Then, came organized cybercrime. Rings of cybercriminals and organized fraud emerged in a coordinated manner so that the chances of getting caught were diminished and more profit could be gained at once. Usually, these cybercriminal organizations would move shipments from a merchandiser to a location that was accessible to them, and then would sell them to a third party for more profit. Similarly, they may also use false websites that require a user to give in personal information so that they can then use them to purchase goods.

As seen from the diagram below[11], internet fraud has only increased in recent years. Even nowadays, Fraudsters and organized crime organizations continue to develop new techniques to gather civilians' personal information while avoiding being uncovered by the complex security systems that are put in place. Some of the most commonly used methods are now: Email spams, Tax fraud, and at times lottery fraud.



Major Countries and Organizations Involved

United States of America- The United states of America, containing the headquarters of some of the largest banks in the world- Such as the World Bank- is one of the largest sufferers of internet fraud. Throughout the COVID-19 pandemic, fraudsters have cost the United States over $4.3 billion dollars financially[12]

FBI- The FBI is the primary law enforcement agency that tackles any issue in regards to internet fraud in the United States. It has established an entire branch of the agency, the Internet Crime Complaint center, which serves to receive complaints from any victims of internet fraud.

- https://www.fbi.gov/investigate/cyber

UN office of drugs and crime- The department within the United Nations that was formed to tackle any form of cyber-related incidence. It is the headquarters that every member state must report to if they contain any data in regards to cybercrime.

- https://www.unodc.org/unodc/index.html

China- China possesses one of the largest populations of online consumers and shoppers globally[13]. Thus, the chinese market is extremely attractive for fraudsters, since they have some of the highest rates of success. This makes the country one of the most targeted worldwide, and is the cause of billions of dollars lost in revenue each year.

Brazil- Brazil contains some of the largest populations of pickpocketers and internet scammers worldwide, as it is said that between 3-6 fraudulent transactions are made each minute[14]. Each year the totalled amount of revenue loss can reach up to $70 billion dollars.
Mexico- Out of the $480 million dollars of lost revenue reported by Mexican banks, 48% of revenue loss cases were caused by credit card frauds[14]. This is because the country's poor cybersecurity measures and large ecommerce market make the Mexican population an exceptionally attractive audience to fraud. Not only is it easier to go undetected, but there are poor systems in place to track down fraudsters.

[12] https://www.voanews.com/usa/fbi-surge-internet-crime-cost-americans-42-billion
[13] https://www.tandfonline.com/doi/abs/10.1080/15564886.2020.1838372?journalCode=uvao20
[14] https://www.builderfly.com/what-countries-have-the-highest-fraud-cases-for-ecommerce/

South Africa- Since over 63% of the South African population prefers online commerce, fraud rates in the country have skyrocketed in recent years. In fact, a study has found that the Fraud rates in the country are currently 10 times higher than the collective amount worldwide.

Romania- Several nations, such as the United States of America, have advised online retailers to prevent shipping goods to Romania due to its dangerously high rates of internet fraud. In the past two years, a total of 12.3 romanian lei has been lost due to scamming, which totals to almost $3 million dollars.

Relevant UN Resolutions and Reports

In a General Assembly resolution created in 2011, (**Resolution 65/230)** the United Nations called for member states to collaborate and initiate a comprehensive study designed to investigate cybercrime problems at the time[15]. This was done so that appropriate measures could be taken against the issue in later resolutions.

In the same resolution, the United Nations called for the office on drugs and crime to aid the member states in the initiation of their cybercrime study. This was done through offering proper training of authorities on the detection and prevention of cybercrime, supplying the adequate technology, and assisting financially.

In a later resolution, (**Resolution 67/189**) the United States praised the intergovernmental group on their cybercrime studies[16]. Their current findings were then presented to the Commision on Crime Prevention and Criminal Justice later that year so that the data could be analyzed and better understood.

Then, several measures were suggested in the resolution to strengthen international cooperation when tackling cybercrime. For example, the findings were translated into six different languages, and several other Crime Prevention and Criminal Justice conventions were planned across different countries to discuss the issue.

Another resolution **(Resolution 22/8)** was created for the sole purpose of 'Promoting technical assistance and capacity-building to strengthen national measures and international cooperation against cybercrime'[17] In this resolution, clauses mentioned improving relations and cooperation

[15] https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/230
[16]https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-7.pdf
[17]https://www.unodc.org/documents/commissions/CCPCJ/Crime_Resolutions/2010-2019/2013/CCPCJ/Resolution_22-8.pdf

between member states and the office on drugs and crime, assigning the department as the headquarters of any gathered data surrounding cybercrime, and invited member states to provide extra budgetary resources to countries in need of so.

Since then, an additional 10 United Nations resolutions have mentioned, discussed, and taken action on cybercrime.

Previous Attempts at Resolving This Issue

In the early 2000s when internet fraud first began to terrorize ecommerce, merchants launched their first security measure- Customer accounts. Up until said point, customers would simply pay their transactions in a one-time visit and not have to give any sort of other personal information. The problem with this, however, was that merchants could not validate that any information was legitimate, and thus fraud was common. With customer accounts, any consumer wishing to purchase a good would have to give in their name, personal email address, and home address if they wished to go through with purchases. These accounts were then also protected by personal passwords and usernames. As a result, businesses could inspect the legitimacy of their customers before any transaction was completed, which made it much more difficult for fraudsters to get away with using stolen credentials as they would then also have to pose as the owner of said card.

However, this only lasted a small amount of time. Considering that these customer accounts were only protected by personal passwords, soon fraudsters began hacking in order to access their credit card information so that they could be used in other fraudulent activities. They could easily change the shipping address of goods, make dozens of purchases, or change the credit card information on their own ‘customer accounts’ to that of the hacked individual’s.

Following the military identity theft incident in the mid 2000’s governments began concealing more personal details of civilians in order to make it more difficult to ‘pose’ as a certain individual. This would also make it easier for merchants to spot fraudulent transactions, since fraudsters would have to use false names and said information could be checked for. It also ensures that certain discounts could not be taken advantage of, something which improved profit for merchants and businesses.

Another attempt at resolving the issue stemmed around punishment. Though it can vary greatly from country to country, most governments made internet fraud a capital offense that can be punished with both large fines and jail time. Not only so, but internet fraud is usually not considered a single stand-alone crime, like for example with murder, yet is one that involves

several crimes. As a result, the jail sentences can be extremely long. In the United States, for example, internet fraud can lead to 20 years in federal prison, as well as a fine of $1 million dollars[18]. A single case of an email scan is enough to convict an individual of this offence, and allows them to serve the sentence if found guilty.

This was done in effort to diminish the number of fraudsters and scammers in countries, as it was hoped that people would not be willing to take the risk of getting convicted of the crime. However, it only pushed for fraudsters to develop more technology so that the chances of their identity being discovered was diminished greatly. As a result, internet fraud remained an issue, yet it only made it more difficult to track down cybercriminals.

Possible Solutions

Considering the urgency of the issue and the plan to eradicate cybercrime on a global scale, delegates must establish measures that benefit all member states. Not only so, but the solutions must tackle a range areas in a society- such as government, civilians, ect. Thus there should be a wide variety of approaches when determining how to tackle the issue.

Some examples of possible solutions can include:

Increased education- It can be argued that with proper education on the dangers of cybercrime from a young age, the crime rates will naturally reduce. Considering the fact that our society now becomes dependent on technology early in childhood, teaching young audiences on how scammers typically target their victims can diminish fraudsters' success rates. Additionally, teaching how to maintain personal information securely can also prevent hackers from accessing personal details.

Increased funding for internet security- With an increased amount of funding, specifically from more developed countries, tighter security systems can be developed for developing countries with higher rates of cybercrime- For example, Mexico. This would then decrease the cybercriminal population within these nations and decreases the number of targeted civilians.

Banning/abolishing VPNs- Considering the fact that VPNs are easily accessible to the public, and that they allow a user to change their device's IP address within seconds, banning this tool could easily prevent cybercriminals from remaining anonymous. Not to mention that it would

[18] https://www.greghillassociates.com/what-is-internet-fraud-the-defenses-the-punishment.html

also make the process easier for authorities to track down fraudsters and charge them with the crime they are guilty of.

Government-verified ecommerce websites- With a law that requires governments to verify the legitimacy and legality of any ecommerce websites that arise, the chances for 'dummy websites' to plague the internet would be greatly diminished. This would eradicate one of the most reliable ways for fraudsters to scam and gather the credentials of civilians within a country and would make the world of ecommerce a much safer and more reliable industry.

Bibliography

The Fraud Practice; Fraud Library - History of Credit Card Fraud,

www.fraudpractice.com/fl-fraudhist.html.

Chen, James. "What Is Tax Fraud?" *Investopedia*, Investopedia, 19 May 2021,

www.investopedia.com/terms/t/tax-fraud.asp#:~:text=Tax fraud occurs when an,paying the entire tax obligation.

"Cybercrime." *Wikipedia*, Wikimedia Foundation, 12 Aug. 2021,

en.wikipedia.org/wiki/Cybercrime#:~:text=Cybercrime is a crime that,someone's security and financial health.

"Cybercriminals." *Definition*, www.trendmicro.com/vinfo/us/security/definition/cybercriminals.

"FBI: Surge in Internet Crime Cost Americans $4.2 Billion." *Voice of America*,

www.voanews.com/usa/fbi-surge-internet-crime-cost-americans-42-billion.

"Facts Statistics: Identity Theft and Cybercrime." *III*, www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime.

"Identity Theft." *Wikipedia*, Wikimedia Foundation, 10 Aug. 2021, en.wikipedia.org/wiki/Identity_theft.

"Internet Fraud." *FBI*, FBI, 31 May 2016, www.fbi.gov/scams-and-safety/common-scams-and-crimes/internet-fraud#:~:text=Internet fraud is the use,the Internet through various methods.

Leonhardt, Megan. "Online Fraud Attempts Are up 25% in the US-Here's Why." *CNBC*, CNBC, 4 June 2021, www.cnbc.com/2021/06/03/why-online-fraud-attempts-are-up-25percent-in-the-us.html.

"Lottery Fraud." *Wikipedia*, Wikimedia Foundation, 26 Jan. 2021, en.wikipedia.org/wiki/Lottery_fraud#:~:text=Lottery fraud is any act,of their legitimately won prize.

"Online Fraud Victimization in China: A Case Study of Baidu Tieba." *Taylor & Francis*, www.tandfonline.com/doi/abs/10.1080/15564886.2020.1838372?journalCode=uvao20.

S.A., Torrance. “What Is Internet Fraud? The Defenses? The Punishment?” *Redondo Beach, California Internet Fraud Lawyers Greg Hill & Associates*, www.greghillassociates.com/what-is-internet-fraud-the-defenses-the-punishment.html.

“United Nations Official Document.” *United Nations*, United Nations, www.un.org/ga/search/view_doc.asp?symbol=A/RES/65/230.

“Universal Declaration of Human Rights.” *Wikipedia*, Wikimedia Foundation, 21 July 2021, en.wikipedia.org/wiki/Universal_Declaration_of_Human_Rights.

“What Countries Have the Highest Fraud Cases for Ecommerce?” *Builderfly Ecommerce Platform to Sell Online & Grow Business*, www.builderfly.com/what-countries-have-the-highest-fraud-cases-for-ecommerce/.