The use of technology to counter frauds and scams for the benefit of society: a detailed study

Sharma, Devashish

16 October 2022

The Use of Technology to Counter Frauds and Scams for the Benefit of Society: A Detailed Study

Devashish Sharma

Amity University Madhya Pradesh, Gwalior

E-mail: devashish.sharma@s.amity.edu

Abstract

With the advent of the digital age, humanity has gained a number of benefits, such as the internet, mobile technology, and crypto currencies. Nevertheless, this has also allowed criminal strategies to evolve and spread as a result of this development. As a result, fraud attempts have increased from analog to digital as a result of the move from analog to electronic methods. When scams and fraud are present in society, there is a reduction in the ability of the government to provide its citizens with the services they need and to support them at the same time. Fraud results in a loss of dollars which could have been invested in healthcare, education, economic development, or public safety if these dollars had not been lost to fraud. The term "Digital Fraud or Digital Scams" refers to the use of a computer or a mobile device, along with the various means of communication available on the internet, by criminals who intend to deceive or harm a company, or an individual, in order to gain financial gain through digital fraud. Organizations need to update outdated analog technology that has been repurposed for digital applications in order to remain competitive against scams and frauds. As we move into a new digital world where we live in today, companies and governments will need to take a fresh look at their authentication procedures.

Keywords: *Fraud, Internet, Authentication Procedures, Analog technology, repurpose digital application, Scam*

Introduction

It is now a prevalent fact in the internet age that there are people involved in frauds and scams more than they used to be as a result of the proliferation of these types of crimes. A growing number of frauds and scams pose a threat to long-standing institutional bulwarks against misinformation, since they are eroding long-standing institutional barriers to misinformation. The severity of this issue has caused worldwide concern regarding this issue. Although these concerns have been raised, it remains to be seen whether individuals, institutions, and societies can be manipulated by malicious actors despite these concerns. Even though these concerns have been raised, they have not been addressed. We must implement a new system of safeguards as soon as possible in order to prevent future frauds and scams. A number of social science and computer science studies have examined how frauds are perpetrated and spread. The researchers have also studied the mechanisms involved in the scams. Despite the fact that fraud and scam have a long history, we would like to draw attention to the scientific questions that remain unanswered despite the proliferation of its most recent, politically motivated forms. Even though fraud and scam have been combated for centuries, there are still many scientific questions that remain unanswered.

There are many ways in which businesses and organizations make use of artificial intelligence. A wide range of financial services firms, including accounting firms, use it to detect fraud in order to detect losses.

There has been an increase in access to data as a result of the transition from working in person to working from home. According to Boston Consulting Group, fraud affected 58% of all businesses globally in 2021. As reported in the McKinsey report for 2021, consumers reported more than 4.9 billion dollars worth of fraud in the year 2021. This is an increase of 69% over the previous year. It was found that online shopping fraud as well as imposter scams accounted for most of these scams.

Impact of Fraud and Scams

In a Mckinsey study, it has been estimated that traditional identity fraud losses, which are the result of criminals unlawfully using the victims' information to steal money, will increase to $50 billion (USD) between 2020 and 2023, an alarming 68% increase from 2019. In addition, the number of adults affected by traditional identity fraud in the United States has increased by more than 49%, reaching more than 21 million individuals. According to the study, there has been an increase in losses from identity fraud scams as well. Generally speaking, these types of losses occur when a fraud operator has been able to manipulate the victim so that he or she divulges sensitive personal information. As a result of this, an additional $30 billion in losses were incurred, which affected an additional 30 million U.S. adults. Over the past few years, the United States has lost a total of $60 billion in the form of identity fraud, which is the result of fraudulent activities involving 50 million Americans.

Fraud can be a traumatic experience for anyone who is victimized by it. Fraud is often the biggest threat to those who are most in need of government services, such as the elderly, the vulnerable, the sick, and the economically disadvantaged. These victims can be severely adversely affected by fraud and suffer a number of detrimental effects as a result. The disadvantage, vulnerability, and inequality that they face can be exacerbated by it. Besides creating lasting psychological and physical trauma for victims, fraud can also have irreversible effects on the families and communities of those who have been victimized.

There is no doubt that criminals will take advantage of stolen consumer information in the wake of the meteoric rise of account fraud. This is done so as to extract as much financial gain as possible from the situation. Due to this, resolving the issues of victims has become more difficult as a result of this. There has also been a negative impact on the victims as it has added time and expense to what has already been a difficult and exhausting experience for them. There has also been a complexity in the resolution process as a result of it. It has been shown that when those over the age of 70 did report money lost to fraud, their average loss was far heftier than that of those under the age of 70. It has been reported that people between the ages of 70-79 have spent a median amount of $800, while people aged 80 and over have lost a median amount of $1,500. The median loss reported by young people between the ages of 20 and 29 was $500 on average.

Social Engineering and Scams

Despite the fact that computer scams use technology, they actually work by using a lot of the same techniques as scams that occur in the real world. Researchers refer to this as 'social engineering' in which the scammers manipulate people's general thought patterns and behavior in order to obtain sensitive information or to hand over money by manipulating how they think and

behave. They also get them toys or give them access to computers or data that they should not be able to access.

To launch a social engineering attack, an attacker uses human interaction (social skills) as a means of obtaining or compromising information about an organization or its computer network through the use of human interaction. An attacker may appear unassuming and respectable, even claiming to be a new employee, repair person, or researcher in order to appear as unassuming and respectable as possible. It is also possible for them to offer credentials to support their claim. It is possible, however, that he or she can gather enough information if he or she asks the right questions, so as to infiltrate an organization's network if he or she asks the right questions. When an attacker is unable to gather enough information from one source, he or she may contact another source within the same organization if one source does not provide enough information. As a result, the attacker may be able to add credibility to their plan by relying on information that comes from the first source.

It is important to understand that scams and frauds are a type of social engineering attack that use email, phone calls, social media, and other methods of personal communication in an effort to trick individuals into providing sensitive information. Information such as Personally Identifiable Information (PII), Financial Information, or Login Credentials may be included in this category. It's possible that the attacker can use this information to gain access to online accounts, personal data, or other details in order to conduct malicious attacks against individuals or organizations. In addition to these phishing scams, there are other forms of phishing that aim to deliver malware to the end user's system, typically by opening malicious attachments or visiting malicious websites.

Technology to counter frauds and scams

It is becoming increasingly common for modern technologies such as big data and artificial intelligence to be used as part of the fight against internet fraud. A new report indicates that it is urgent that fraud and scams are countered as new cases of mobile and online fraud are posing a threat to the safety of personal information and social stability in the coming years. Globally, consumers have actively used online shopping and innovative online payment services during the COVID-19 pandemic this year, however many have also been defrauded during their online transactions, according to a report released by Boston Consulting Group today. Consumers between the ages of 20 and 29 are more likely to encounter telecom and online fraud than any other group of consumers.

We have to understand that ecommerce refers to commercial transactions that are conducted electronically over the Internet, usually through an online store, when we talk about ecommerce. The most common devices used for this type of transaction are desktop computers, laptops, tablets, and mobile phones. Fraud can be defined as a criminal act involving the deception of an individual or group with the intent of gaining financial or personal gain.

The term "ecommerce fraud" refers to the criminal act of deception that is committed during a commercial transaction over the Internet with the aim of gaining some financial or personal gain for the fraudster while adversely affecting the bottom line of the merchant in the process. There are two types of ecommerce fraud: payment fraud and ecommerce fraud.

In addition to its relation to the internet, cybersecurity also takes into consideration personal safety as well as social stability. According to a report by McKinsey, internet security risks, including telecom scams, fraud messages and malicious websites, should remain on the public's radar.

There will be an increase in demands for cybersecurity and privacy protection with the introduction of emerging technologies such as artificial intelligence and 5G.

Recommendation

It is strongly recommended by the author that you never click on links or open attachments delivered by unexpected or unsolicited emails, social media messages, or text messages sent to you. Whenever you accidentally click on a suspicious link or visit a phishing website, you should not enter any personal information and disconnect your device from the network as soon as possible. You should run a full scan of your system using your antivirus software. To prevent the spread of malware on a work computer, contact your IT help desk immediately so that the system or device can be evaluated and quarantined as needed. Monitor your bank accounts, credit profiles, and other online accounts if you entered or divulged personal information. You should contact the company mentioned in a suspicious email and forward the email to them for verification. Additionally, please refrain from replying to spam emails, as this only confirms to the sender that your email account is active. The email should be deleted instead. Last but not least, make sure you use up-to-date antivirus software and firewall protection to prevent phishing attacks, and enable multi-factor authentication (MFA) for all accounts that offer it to greatly reduce your risk of account compromise. Organizations can prevent incidents resulting from phishing attacks by training and educating their employees.

Conclusion

There is no doubt that consumers are at risk of being scammed online, but they are not the only ones who are at risk of being scammed. Due to recent data breaches at major retailers and government agencies, as well as increasing incidents of fraudulent emails, businesses and governments are increasingly vulnerable to email and internet scams and fraud. Both consumers and businesses should take precautions to ensure their online security. These precautions also apply to the government. Cybercrime is a global epidemic. It is true that the Internet has opened up a whole host of new opportunities for scams and fraud. The internet is rife with fraudulent activities in the form of online shopping, social media, and even dating sites. It is common knowledge that users have access to the internet and mobile devices, but how educated are they when it comes to internet and mobile scams and cybercrime? Scammers use a variety of different tactics to attempt to defraud their victims. In addition, even though advanced technology helps us all, it also opens up new avenues for cybercriminals to exploit. The only way to be able to avoid scammers completely is to learn how they work, how to avoid them, and spread public awareness about them at the same time.

It is no secret that mobile devices and Internet access have become some of the most popular tools used by criminals to commit fraud and they are becoming more and more sophisticated with the ways in which they are utilizing their hacking techniques in order to do so. This is why it is extremely important for consumers to use only trusted and secure wireless networks when conducting their financial transactions online and to be aware of the possibility that any personal information they share online can be used by fraudsters to commit online fraud on them.

References

Albrecht, W. Steve, et al. Fraud examination. Cengage Learning, 2018.

Baisya, Rajat K., and Siddhartha Paul Tiwari. "E-governance Challenges and Strategies for Better-managed Projects." *Emerging Technologies in E-Government* (2008): 203-208.

Bansal, Sanchita, Isha Garg, and Gagan Deep Sharma. "Social entrepreneurship as a path for social change and driver of sustainable development: A systematic review and research agenda." *Sustainability* 11.4 (2019): 1091.

Bierstaker, James L., Richard G. Brody, and Carl Pacini. "Accountants' perceptions regarding fraud detection and prevention methods." Managerial Auditing Journal (2006).

Calvo, Sara, et al. "Educating at scale for sustainable development and social enterprise growth: The impact of online learning and a massive open online course (MOOC)." *Sustainability* 12.8 (2020): 3247.

Cukier, Wendy, et al. "Social entrepreneurship: A content analysis." *Journal of Strategic Innovation and Sustainability* 7.1 (2011): 99-119.

Macke, Janaina, et al. "Where do we go from now? Research framework for social entrepreneurship." *Journal of cleaner production* 183 (2018): 677-685.

Mair, Johanna, and Ignasi Marti. "Social entrepreneurship research: A source of explanation, prediction, and delight." *Journal of world business* 41.1 (2006): 36-44.

OECD| European Commission. "Policy brief on scaling the impact of social enterprises: Policies for social entrepreneurship." (2016).

Pearce, Joshua, et al. "Leveraging information technology, social entrepreneurship, and global collaboration for just sustainable development." (2019).

Popov, Evgeny V., A. Yu Veretennikova, and Kseniya M. Kozinskaya. "The sharing economy and social entrepreneurship for sustainable development." *Changing Societies & Personalities. 2022. Vol. 6. Iss. 1* 6.1 (2022): 98-122.

Siddhartha Paul Tiwari., and Baisya, Rajat K. "E–governance and its impact on enterprise competitiveness: Trends, Status and Challenges." *MDI, Gurgaon INDIA in Association with Australian Centre for Asian Business, University of South Australia, Adelaide, AUSTRALIA* (2014): 1.

Tiwari, Siddhartha Paul. "Workshop on Digital Marketing: Credit Course, IIM, Indore (2010): 1-24.

Tiwari, Siddhartha Paul. "Editorial: Project and Technology Management Foundation (PTMF) Newsletter (December, 2014)" *3-1*(2014).

Tiwari, Siddhartha Paul. "Exploring the Linkage between a Successful Digital Campaign and Gaming." *Casual Connect, Asia Pacific, Singapore* 1 (1) (2014): 5-6.

Tiwari, Siddhartha Paul. "Business: Innovation & Survival, by a Googler." (2015).

Tiwari, Siddhartha Paul. "Strengthening E-Commerce Product Launches-Improving Efficiencies from Development to Production." *Project And Technology Management Foundation (A Non-Profit Organization) Member of Asia Pacific Federation of Project Management* 1.2 (2015): 4-6.

Tiwari, Siddhartha Paul. "Editorial: Project and Technology Management Foundation (PTMF) Newsletter (June, 2015)" *3-1*(2015).

Tiwari, Siddhartha Paul. "Strengthening E-Commerce Product Launches-Improving Efficiencies from Development to Production." *GMM Content Creators Workshop on Countering the Narrative of Violent Extremism - Kuala Lumpur, Malaysia* (2015).

Tiwari, Siddhartha Paul. "Diversity and its importance in today's corporate environment." *https://dms.iitd.ac.in/guest-speakers/* (2015): 1.

Tiwari, Siddhartha Paul. "Emerging trends in soybean industry." (2017).

Tiwari, Siddhartha Paul, and S. P. Tiwari. "Is export-oriented and currency dynamics-based Indian soybean revolution environment-friendly." *Current Science* 114.08 (2018): 1604-1605.

Tiwari, Siddhartha Paul. "Emerging Technologies: Factors Influencing Knowledge Sharing." *World Journal of Educational Research* (2022).

Tiwari, Siddhartha Paul. "Information and communication technology initiatives for knowledge sharing in agriculture." *arXiv preprint arXiv: 2202.08649* (2022).

Tiwari, Siddhartha Paul. "Knowledge Enhancement and Mobile Technology: Improving Effectiveness and Efficiency." *arXiv preprint arXiv: 2208.04706* (2022).

Tiwari, Siddhartha Paul. "Knowledge Management Strategies and Emerging Technologies--An Overview Of the Underpinning Concepts." *arXiv preprint arXiv: 2205.01100*(2022).

Tiwari, Siddhartha Paul. "Re-emergence of Asia in the New Industrial Era." *Technium Soc. Sci. J.* 29 (2022): 471.

Tiwari, Siddhartha Paul. "Organizational Competitiveness and Digital Governance Challenges." *Archives of Business Research* 10.3 (2022).

Tiwari, Siddhartha Paul. "The Potential Impact of COVID-19 on the Asian Rural Economy: A Study Based on Asian Countries." *Journal of Education, Management and Development Studies* 2.3 (2022): 1-7.

Tiwari, Siddhartha Paul. "Covid-19: Knowledge Development, Exchange, and Emerging Technologies." *International Journal of Social Science Research and Review* 5.5 (2022): 310-314.

Tiwari, Siddhartha Paul. "Knowledge Management Strategies and Emerging Technologies-an Overview of the Underpinning Concepts-Siddhartha Paul Tiwari." (2022).

Wang, Xueqin, et al. "How can the maritime industry meet Sustainable Development Goals? An analysis of sustainability reports from the social entrepreneurship perspective." *Transportation Research Part D: Transport and Environment* 78 (2020): 102173.

Weerawardena, Jay, and Gillian Sullivan Mort. "Investigating social entrepreneurship: A multidimensional model." *Journal of world business* 41.1 (2006): 21-35.

Wilhelm, Wesley Kenneth. "The fraud management lifecycle theory: A holistic approach to fraud management." Journal of economic crime management 2.2 (2004): 1-38.