Career Point International Journal of Research (CPIJR)
©2022 CPIJR | Volume 2 | Issue 1 | ISSN : 2583-1895

ONLINE SCAMS – A CRISIS IN ONLINE WORLD

Diynash Malav[1], Shalini Chawla[2]

[1]School of Computer Applications, Career Point University, Kota

[2]Assistant Professor, School of Computer Applications, Career Point University, Kota

Abstract Millions of people have fallen victim to a wide variety of online scams, many of which are conducted entirely or partially online, making internet fraud a big issue in many nations. The scope and character of this issue are examined in this article. based on information gleaned from in-depth interviews with victims of online fraud, including pharming, phishing emails, tech support scams, and numerous online articles. The article examines the reasons why people fall for internet fraud. It lists a number of factors that contribute to fraud, such as the variety of scams, the tiny sums of money sought, the authority and legitimacy presented by con artists, emotional appeals, embarrassing frauds, pressure and coercion, grooming, fraud at a distance, and many strategies.

I INTRODUCTION

There are various fraud tactics used in the online world. Because of online fraudsters, these frauds are conceivable. Scams can occur in a plethora of different ways, including through phishing emails, social media, SMS messages on your phone, phone calls posing as tech assistance, scareware, and more. These scams' primary objectives can include identity theft, the theft of credit cards, and the capture of user login and password information. With thousands of people losing their hard-earned money in a matter of minutes, it has truly become a severe problem. Such instances occur frequently, and the current state of affairs is exceedingly bleak, with the likelihood of things getting worse in the future increasing.

They cannot be stopped until firm action is taken against these frauds. However, who is in charge of the faceless criminals hiding behind their computers? This is both practically and conceptually impossible. So where is the answer to the problem?

Money orders have become almost obsolete. With the current pandemic situation, cash transactions have reduced to almost zero. Online payments seem to be the thing of the future, one that propels India into the digital age of independence. The Government launched online payments portals, and encouraged online transactions rather than cash transactions, with the slogan- "Make India Digital".

With immense technological boost in the finance and banking sectors of the country, online frauds in India, have increased in number as well. Hackers and scammers are finding more innovative ways to skim off money from law-abiding citizens. The more digital India gets, the more ways scammers find to scam people of their hard-earned money. These are a few common types of online frauds that have been registered by the Cyber Crime cell of India.

Different Methodologies of online fraud

There are different variety of scams in the online world. Since the fraudsters are quick to learn from their errors and make it difficult for the authorities to find them, previous attempts to curb these scams have all failed. This is the reason why these frauds are still prevalent and still wreak havoc on unwary internet users. Following is a list of the common online frauds-

Phishing

Pharming

Fake non-profit donation

Fake anti-virus software

Tech support scams

Identity theft

II LITERATURE REVIEW

Motive behind these scams The primary goal of online scams is to obtain the targets' financial information so that the fraudster can utilise it to transfer any amount of money to their own bank account.
Although the fraudsters' true motivations aren't always evident, their immediate goal is undoubtedly to obtain a sizable sum of money and flee with it as quickly as they can.

The fact that many online users are afraid to confidently browse the Internet is the single factor contributing to the success of these online scams. This is particularly true if they have only recently started using the Internet.

Common online scams explanation

Explanation of the Common Online Scams Due to the complexity of the online scams, it can be hard for a novice Internet use to recognise each and every scam. The large variety of scams makes it even harder for the user to stay away from the traps set in multiple websites. That is why it is necessary to have a sound knowledge about the working of such scams, so that they can be recognised and prevented, if not eradicated entirely

Phishing

This is one of the earliest forms of scams. Phishing refers to the process of creating a fake webpage that looks exactly like the webpage it is mimicking. This is usually a bank or credit card website. The target user is sent a cleverly disguised link through email, causing the user to believe that the email has arrived from the real bank or Credit Card Company. When the user clicks on the link, instead of being led to the original website, the fake website shows up instead. The unsuspecting user enters his/her login credentials into the webpage, which are then sent to the scammer's harvesting page, which is usually a text file, with a script to collect the login credentials Once the login credentials have been entered, the user is then automatically redirected to the original website, being none the wiser about the collection of the login credentials by the fake webpage. This is the basic working of a phishing scam.

III METHODOLOGY

Case study- What happened in the case of the e-mail scam involving ICICI Bank? A few customers of ICICI Bank received an e-mail asking for their Internet login name and password to their account. The e-mail seemed so genuine that some users even clicked on the URL given in the mail to a Web page that very closely resembled the official site.The scam was finally discovered when an assistant manager of ICICI Bank's information security cell received e-mails forwarded by the bank's customers seeking to crosscheck the validity of the e-mails with the bank. Such a scam is known as 'phishing.

Pharming

Pharming is a cyber-attack by which hacker install malicious code on personal computer or server, redirect a website traffic to another without their knowledge or consents. This is also called “Phishing without a lure”. It occurs when hackers locate vulnerabilities in DNS software and by rearranging the host file on the target computer. The term “Pharming” is

neologism based the word "farming" and "phishing". Phishing is a type of social engineering attack to obtain access credentials like username, password. Now a year, both phishing and pharming is used. Now a day for online identity theft both pharming and phishing is used. The most popular pharming targeted website are online banking and e-commerce websites. Due to lack of security administration, Desktop are also vulnerable to pharming threads. Pharming and phishing threads have been used simultaneously and these can cause the most potential for online identity theft. Unfortunately, anti-virus software is incapable of protecting against these types of cybercrime. Pharming attack will redirect the victim to the fake website even though victim enter the correct website address.

Case study-

A spurt in cyber-attacks has left Lucknow police in a tizzy as the database of four companies were targeted and tampered in the last one week. The biggest cyber-attack was reported on March 30 when the website of a Gomtinagar-based company which maintains database of cane farmers' transactions with sugar mills in 12 districts of UP was breached by hackers who either deleted or changed the data of around 19 lakh farmers.

Fake Non Profit Donations (Fake Charity)

Charity Fraud is the act of using deception to get money from people who believe they are making donations towards a cause. Often a person or a group of people will make material representations that they are a charity or part of a charity and ask prospective donors for contributions to the non-existent charity.

Case study-Charity Fraud is the act of using deception to get money from people who believe they are making donations towards a cause. Often a person or a group of people will make material representations that they are a charity or part of a charity and askprospective donors for contributions to the non-existent charity.

Tech Support scams

A technical support scam, or tech support scam, is a type of fraud in which a scammer claims to offer a legitimate technical support service. Victims contact scammers in a variety of ways, often through fake pop-ups resembling error messages or via fake "help lines" advertised on websites owned by the scammers. Technical support scammers use social engineering and a variety of confidence tricks to persuade their victim of the presence of problems on their computer or mobile device, such as a malware infection, when there are no issues with the victim's device. The scammer will then persuade the victim to pay to fix the fictitious "problems" that they claim to have found. Payment is made to the scammer through ways which are hard to trace and have fewer consumer protections in place which could allow the victim to claim their money back, usually through gift cards.

Case study-

Three Indian nationals, who had initially come to Singapore to study, were sentenced to prison for participating in a transnational money mule syndicate that was perpetrating "tech support scams," a media report said.

On Wednesday, Nandi Niladri, 24, was handed the stiffest sentence of 18 months in prison, after he pleaded guilty to three charges under the Payment Services Act and one count of obstructing the court of justice, the Straits Times newspaper reported.

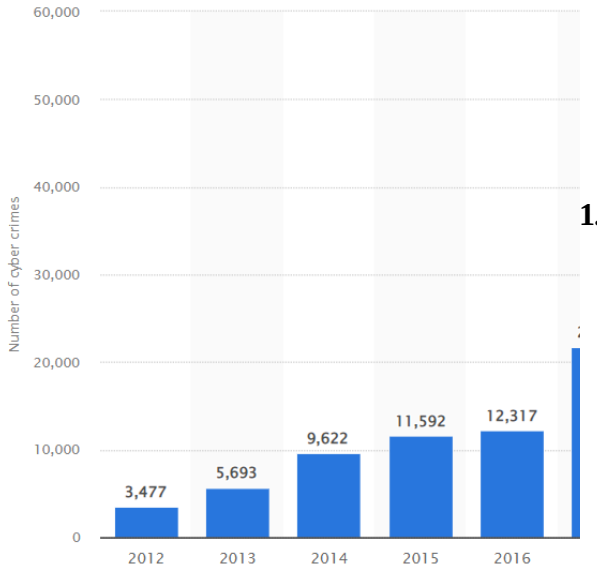
Another man, Akash Deep Singh, 23, who dealt with cash totalling more than SGD 118,000, pleaded guilty to three charges, including an offence under the Act, and was sentenced to a year in jail, the report said.

The third offender, GiriDebjit, 24, was sentenced to seven months' jail after he pleaded guilty to two charges, including an offence under the Act.

He had received multiple inward transfers totalling more than SGD 61,000, it said.
Giri and Nandi came to Singapore to study in 2019, while Akash arrived the following year. Court documents, however, did not disclose details of the colleges they were studying in.
The trio were the last offenders linked to the case to be dealt with in court.

IV RESULT

Chart to Express Cases in India



India saw a significant jump in cyber crimes reported in 2020 from the previous year. That year, over 50 thousand cyber crime incidents were registered. Karnataka and Uttar Pradesh accounted for the highest share during the measured time period.

Uttar Pradesh leads the way

The northern state of Uttar Pradesh had the highest number of cyber crimes compared to the rest of the country, with over six thousand cases registered with the authorities in 2018 alone. India's tech state, Karnataka, followed suite that year. A majority of these cases were registered under the IT Act with the motive to defraud, or sexually exploit victims.

It's a numbers game

It was estimated that in 2017, consumers in India collectively lost over 18 billion U.S. dollars due to cyber crimes. However, these were estimates based only on reported numbers. In a country like India, it is highly likely that the actual figures could be under-reported due to a lack of cyber crime awareness or the mechanisms to classify them. Recent government initiatives such as a dedicated online portal to report cyber crimes could very well be the main factor behind a sudden spike in online crimes from 2017 onwards.

Measure To Prevent Getting Scammed In Online World

1. **Use verified apps only-**

Mobile apps have changed the way we shop and transact. Every time you install an app on your device, make sure you are using a verified app. Whether it's a financial app or a new game, download only from official play stores like Google Play Store, Windows App Store or Apple App Store.

2. **Use secure connections only-**

The urge to use free Wi-Fi at a cafe, hotel lounge or airport can also lead to financial fraud. Avoid using public hotspots for making a financial transaction. Public networks are more prone to the risk of data theft since their encryption can be cracked easily to access your account's crucial information.

3. Browse on authorised websites only-
Beware of imposter websites that may look professional or carry the same domain name as the original one in the URL. Look for "https://" before "www" and the lock icon on the address bar of your browser.

4. **. Be vigilant while using card-**

Always make a card payment in front of your eyes. Be sure that the POS machine is 100 percent genuine. There are dozens of stories about cards being cloned by skimmers since the card was out of sight while the transaction was being done. Don't let anyone steal your hard-earned money because of your negligence.

5. **Don't compromise on security software for phones/computers-**

Everyone wants their payments to be secure but how many of you pay attention to your mobile and computer's security software, web browser and operating system. Update your PC/laptop and mobile security to prevent online mishappenings. Also, always set up strong passwords with a combination of special characters, letters, numbers and upper and lowercase. Don't forget to change the passwords on a regular basis

6. **Don't share personal information with anyone-**

Never share your personal information online or offline, unless you are absolutely sure about the authenticity of the representative. There can be a possible scammer hiding behind a stranger or any third party posing as an executive from a bank or financial institution. Always verify the identity of the person asking for your financial details. Bank authorities never ask for sensitive information like OTP, CVV on calls. Also, sharing important financial details like bank name, branch, account number, etc on social media is a big no.

Perience Link baiting, spurious emails and SMS are the most common forms of trapping people into fraud. These links may seem genuine and attract your attention with claims of lottery or a job overseas. Do not follow any such links, as they may lead you to a phishing site and rob you off your mobile's security features. It's better to hang up in case you receive an unsolicited call.

7. **Never click on suspicious links on SMS or emails**

Every year, thousands of people fall prey to banking scams with the internet becoming one of the most popular tools to commit fraud. These basic measures can help you protect yourself from being a victim of online fraud.

In case your debit or credit card is lost or stolen, informing the bank immediately and getting it blocked is the first step to avoid a financial loss. Timely blocking the card can save your financial security from being compromised.

V CONCLUSION

Although it is impossible to curb all forms of online scams in the near future, it is indeed possible for the average netizen to be safe from the dangers of such scams, by staying away from them. This might surely appear to be a challenge, and it will take some time to recognise and educate netizens about all such scams. However, for a smooth browsing experience, it is indeed essential that the netizens first learn about these scams, so that they can then proceed to have an uninterrupted browsing ex

VI REFERENCE

[1] Applegate, S. D. (2009). Social engineering: Hacking the wetware. Information Security Journal, 18, 40-46.

[2] Bardzell, J., Blevis, E., & Lim, Y. (2007). Human-centered design considerations. In M. Jakobsson, & S. Myers (Eds.), Phishing and countermeasures (pp.

241-259). Hoboken, New Jersey: John Wiley & Sons, Inc.

[3] BBC News (2004). Suicide of internet scam victim.

[4] http://news.bbc.co.uk /2/hi/uk_ news/ England / cambridgeshire/3444307.stm

[5] Blommaert, J., & Omoniyi, T. (2006). E-mail fraud: Language, technology, and the indexicals of globalization. Social Semiotics, 16, 573-605. doi:10.1080/10350330601019942

[6] Brandt, A. (2006). How bad guys exploit legitimate sites (electronic version). PC World, 24, 39.

[7] Capaldi, N. (1971). The art of deception. New York: Donald W. Brown Inc.

[8] Carey, L. (2009). Can PTSD affect victims of identity theft: Psychologists say yes. http://www.associatedcontent.com/article/2002924/ can_ptsd_affect_ victims_of_identity.html

[9] Emigh, A. (2007). Mis-education. In M. Jakobsson, & S. Myers (Eds.), Phishing and countermeasures (pp. 260-275). Hoboken, New Jersey: John Wiley & Sons, Inc.

[10] Gilbert, D. T., & Malone, P. S. (1995). The correspondence bias. Psychological Bulletin, 117, 21-38. doi:10.1037/0033-2909.117.1.21

[11] Gulati, R. (2003). The threat of social engineering and your defense against it. SANS Institute InfoSec Reading Room. http://www.sans. org/rr/papers /index. php? id=1232

[12] Krishnanjali Magade and Dr. Amit Sharma "Prediction Accuracy On Automating Of Overnight Patient Care" Advanced Engineering Science ISSN: 2096-3246 Volume 54, Issue 02, August, 2022

[13] Harley, D., & Lee, A. (2009). A pretty kettle of phish. ESET antivirus and security white papers. http://www.eset.com/download/whitepapers/Phishing Online.pdf

[14] Shipra Gupta, Dr. Amit Sharma. A predictive approach for speaker verification by machine learning and MFCC. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1296-1299

[15] Dr. Amit Sharma. 4g wireless technology and its standards taking consideration evolution of 4g technology. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1102-1105

[16] Seema Kumari Nagar, Dr. Amit Sharma. An effective multi user setting schemes. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1090-1091

[17] Dr. Amit Sharma. Development of android application services at Arokia and its architecture. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1072-1075

[18] Dr. Amit Sharma. Implementing the design of service oriented architecture. National Journal of Multidisciplinary Research and Development, Volume 3, Issue 1, 2018, Pages 1027-1030