Factor and Types of Scam Websites

Gulshan
Student,
School of Computer Science & Engineering,
Lovely Professional University, Phagwara, Punjab, India.

Abstract: Digital Scams through Scam websites are consistently increasing year by year. Cyber fraud/scam happens due to people's carelessness or if they get deceived by someone. Scammers come out with new methods to fool common people and scam small or large sums of money through them. The scope of this review paper is to throw light of different kinds of online scam websites and factors which lead to online scam. This paper also discusses the scope of components of scam websites and pattern analysis which is used to scam victims online

Index Terms **- scam-website, scammer, scam.**

I. INTRODUCTION

With the rise of internet services and activities, many scam websites [1] are emerging for the sole purpose of stealing sensitive information or money out of poor and uninformed victims. The Internet is now used for the majority of tasks, and for services, and businesses, including shopping, banking, logistics, entertainment, and personal needs, are turning online. And this opens doors for hackers, scammers, and fraudsters.

Where scam websites operate for the sole purpose of making victims using online methods by certain tactics and methodologies. A number of scam websites operate with the account to factor that they seem too good to be true and offer ridiculous offers or experiences which are far ahead of reality. With such questionable offers and deals, an average internet user falls into the scam website's trap and loses either sensitive information or digital cash

II. ANATOMY OF ONLINE SCAM WEBSITES

2.1 Seems Too Good To Be True

Scam websites have a tendency to impose themselves as authentic and an official entity to lure victims into sweeping personal sensitive information or money out of their bank accounts. Online scam websites provide services or products at price or terms which seem too good to be true.

2.2 Urgency For Victim To Do Transaction

The scam websites boggle victim mind by projecting un-reliable information such as blockage of credit card or blockage of your bank account. Such information created a panic rush in victims and forced them to pay some amount of money to fix the issue.

2.3 Stealing Personal Info

Personal sensitive information is used by large businesses and companies to find and sort the target audiences with the means of digital marketing. Such information is collected in large databases with the input of various scam websites, which lures victims into sharing personal sensitive information, including choice of interest and physical residential address.

2.4 Stealing Money From Victim

Online scam websites which impose themselves from bank or payment authority for offers, gift cards to failed transaction updates. Such websites offer victims a conventional way to pay their debt in return of offers or gift vouchers.

2.5 Using Social Tactics To Lure Victim

Usage of photos and videos which activates people sentiments are used to make donations on behalf of disabled or financially poor victims. These donations are directly connected to scam websites and are never delivered to people who are represented in such social causes.

III. TYPES OF SCAM WEBSITES

Websites use various tactics to represent themselves as authentic and genuine to collect sensitive information or small amounts from a large sum of individuals. The traffic or communication source of such websites is primarily email and referral links. No matter what age or background, people tend to fall victim to many scam types [2] in the Terrain of Cybercrime

3.1 Lottery Online Scam

These scam websites operate by showing advertisements regarding lottery prize or money winning games to its victims using digital platforms to a large pool of victims. These victims end up giving sensitive information in the hope of getting a lottery or game prize.

3.2 Money-winning Game

Victims pay a small amount to buy virtual coins in order to play money-winning games, which promises to make the victim candidate a huge sum of money in a short period of time.

3.3 Online Dating Scam:

In online dating scam websites, victims are promised false hope of appropriate candidate proposals or recommendations in exchange of a small fee. After victims pay the fee, promised recommendations are not delivered or provided to the victim.

IV. FACTORS AFFECTING ONLINE SCAM

Average internet users are getting awakened about different types of Internet scams [3]. There is no doubt scam websites are getting advanced too. Scammers regularly come up with new strategies and target a new set of people each time. However, the main reason for people getting scammed is the lack of knowledge about technology.

4.1 Education

Uneducated individuals most often fall into such traps and reveal they are true credentials without even thinking straight. At the same time, the educated ones might also get fooled sometimes since scammers are presenting their art of deception in a more genuine way. With the increased frequency of such scams, now students are also a victim of this crime.

4.2 Offer Traps

Different types of links/offers are mostly shared on social media messengers apps by teenagers. Such offers are just a way to make you reveal everything about your financial accounts.

people with low self-control respond differently to deceptive online commercial offers [4] where people who are uneducated tend to fall into such traps easily.

For eg. Get iPhone 11 Pro Max now at just Rs. 5999", "Free Spin - Get a chance to win amazing prizes.

Scam websites target to steal money from the users, who mention their own bank details at such sites without questioning for ones. Once the user places an order on a scam website, the scammers run away with their money without any change of shipping the product or services which was advertised.

4.3 Age Factor

Cellphones and the internet have evolved very recently. And along with this evolution, the rate of scammers and fraudsters are also increasing.

Older adults are disproportionately targeted by various kinds of fraud [5]. As it is quite difficult for the old generation to understand each and every activity and respond accordingly. So, the rate of the victim is more in the age group of 65 - 80 as compared with the age group of 25 - 40.

Students, Women, men, and educated people are likely to be tricked by cyberscams, in general [6]

4.4 Industry Factor

Apart from all the other factors, the industry sector is again an important part of this conversation. Farmers and drivers are highly likely to get tricked by the imposters.

V. INDICATORS OF SCAM WEBSITES

5.1 Domain Age

Scam websites last no longer than 1 month, however some grand scheme of scam website also operates for 6 months. However, all of such websites get in the eye of the criminal/cyber department and shut down immediately under 1 year.

5.2 Flashy Ads

Scam websites uses the concept of flashy and attractive advertisements to lure victims into the cyber scam. Lucrative offers of antique products or expensive products selling for cheap are largely used to scam victims.

5.3 Impersonified name

Imersonified names are used on the website to show similarity with large brand names. For eg. www.amazon4.com personified as www.amazon.com

5.4 No sign-up/ login options

Such websites are made to server one scam page to use. Hence other functional requirements such as sign up, log in, customer care, etc. are not actively present.

5.5 Website navigation

Website involved in online scams tend of have poor or no optimization for a different set of devices.

5.6 Price cut from the market

Websites involved in scam containing selling of products offers expensive products in cheap as compared to current market price in order to loot customers

REFERENCES

[1] : J. Drew and T. Moore, "Automatic Identification of Replicated Criminal Websites Using Combined Clustering," 2014 IEEE Security and Privacy Workshops, San Jose, CA, 2014, pp. 116-123, doi: 10.1109/SPW.2014.26.

[2] A. Stabek, P. Watters and R. Layton, "The Seven Scam Types: Mapping the Terrain of Cybercrime," 2010 Second Cybercrime and Trustworthy Computing Workshop, Ballarat, VIC, 2010, pp. 41-51, doi: 10.1109/CTC.2010.14.

[3] : M. Sharifi, E. Fink and J. G. Carbonell, "Detection of Internet scam using logistic regression," 2011 IEEE International Conference on Systems, Man, and Cybernetics, Anchorage, AK, 2011, pp. 2168-2172, doi: 10.1109/ICSMC.2011.6083998.

[4] : Johan van Wilsem, 'Bought it, but Never Got it' Assessing Risk Factors for Online Consumer Fraud Victimization, European Sociological Review, Volume 29, Issue 2, April 2013, Pages 168–178, https://doi.org/10.1093/esr/jcr053

[5] Jingjin Shao, Qianhan Zhang, Yining Ren, Xiying Li & Tian Lin (2019) Why are older adults victims of fraud? Current knowledge and prospects regarding older adults' vulnerability to fraud, Journal of Elder Abuse & Neglect, 31:3, 225-243, DOI: 10.1080/08946566.2019.1625842

[6] : Whitty, M.T. Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims. Eur J Crim Policy Res 26, 399–409 (2020). https://doi.org/10.1007/s10610-020-09458-z