IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol. 10, Issue.11, November 2022 E-ISSN: 2347-2693

Online Fraud Types and Open-Source Online Fraud Prevention Tools– An Analysis

S. Vijayarani[1*], R. Janani[2]

[1,2]Department of Computer Science, Bharathiar University, Coimbatore, India

*Corresponding Author: vijayarani@buc.edu.in

DOI: https://doi.org/10.26438/ijcse/v10i11.1619 | Available online at: www.ijcseonline.org

Received: 01/Apr/2022, Accepted: 02/Jun/2022, Published: 30/Nov/2022

Abstract – The evolution of the world economy has been very high with the proliferation of new technology and universal communication super highways. Nonetheless, one of the unintended consequences of online or the internet is its use for illegal activities. Increasing social crime has become a global problem, and the activity of international criminal organizations has been steeply increased. Online fraudulent usually denotes to any form of fraud mechanism that uses the internet's one or more components, such as emails, websites, web portals, etc. Nowadays, many tools are available to prevent the users from online fraudulent. The main aim of this paper to discuss the types of online fraud and tools to prevent those fraud activities.

Keywords – Fraudulent Types, Spam, Scam, Phishing, Identity Theft, Spyware, Tools.

I. INTRODUCTION

Internet users are rising day by day and in 2019 they are projected to grasp 627 million people because, the internet is now easy to access from anywhere and low-cost. People can use their smartphones to access the internet. There is also a rapid growth of the internet in rural areas [1]. Even as the majority of people connected to the internet seems to be on the rapid increase, cyber-crime is also on the rise yet this fraud has caused many people to lose their livelihood. A fraud is [2]:

- A misleading assertion of empirical truth
- Proof on the victim's part that the argument is false
- The victim's intention to deceive the presumed victim
- The suspected victim's justifiable relies on the statement
- As a result, it injures the suspected victim

Internet fraud is a kind of fraud which exploits the world wide web. It's not even a single fraud, in that there are innumerable frauds [3]. Internet scammers are here and inventive techniques are developed to exploit people and strip money out of their bank account. Figure 1 shows the tools used for online frauds.

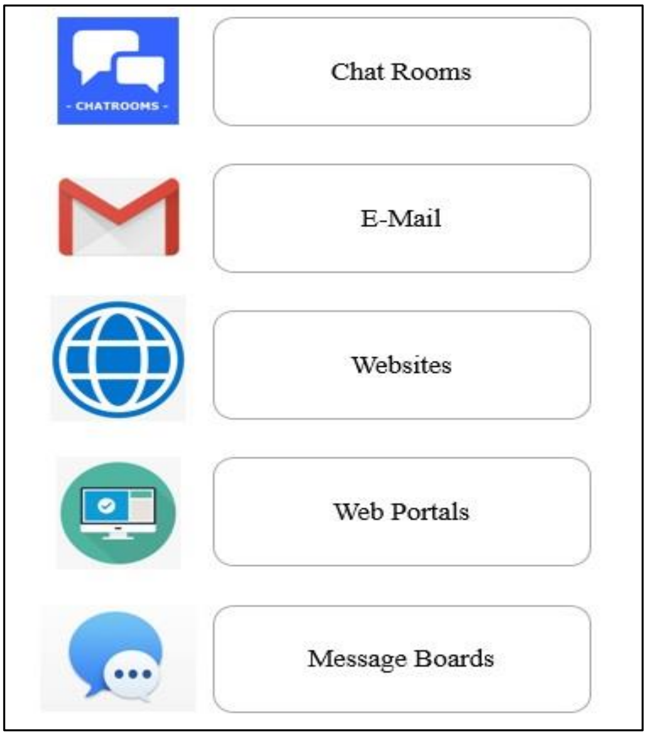

Figure 1. Online Fraud Generation Tools

II. RELATED WORK

In [1], the authors assessed a number of tools and provide suggestions for educational institution. This study, done at the University of the South Pacific, used a four-phased method, commencing with desk research and moving on to pilot testing with the help of both professionals and students. Based on the "survival of the fittest" philosophy, a tool was eliminated in each phase, with subsequent phases building on prior phases' deliverables and milestones. The findings of this inquiry are presented in this report along with some of its major conclusions.

In [2], With an emphasis on the enlarged versatilities of this modern crime, the authors was examined the identity theft from a theoretical perspective. Identity theft components and techniques was broken down for classification, and future discussions will place special emphasis on contemporary changes in online fraud. The study concluded with recommendations for better identity security strategies and consequences of the intimate connections between identity theft and the rapidly expanding Internet.

In [3], the authors were discussed about, how prevalent Internet fraud has become from 1998 to 2002. The variables specifically looked at were the various types of online fraud, the payment methods used to commit those frauds, the victims who were impacted, and any trends. The findings of this study should be interesting to all categories of law enforcement personnel, computer and information system security designers, and notably online system users.

In [4], they were started their work with a straightforward taxonomy of OSN scams before going into detail about each fraud's characteristics and discussed some of the most recent, cutting-edge studies on how to detect them. They emphasized the scope and severity of these frauds whenever they needed. They were recognized the identity manipulation and the spread of false information as two crucial elements in the modus operandi of the majority of OSN frauds.

III. TYPES OF ONLINE FRAUDS

There are several types of fraud which includes [4],

- Spam
- Scam
- Phishing
- Identity Theft
- Spyware

1. Spam

Spam is a standard term used to describe 'Junk mail' or unprompted communications sent to mobile phone or email account. Such notifications overlap, but are empirically different but commercial and often annoying with their volume of text. Today they are among the most significant threats to companies and communities. An email or Notifications is sent demanding the user to access the malicious account and enter their sensitive information, which include access codes for security [4]. The page looks authentic but users who enter information send their information unknowingly to the fraudster. There are many tools are available to prevent the spam fraud and the tools are listed as follows,

Table 1. List of tools to prevent the Spam Fraud

S.No	Tool Name	Description
1.	AntiPhish [5]	It is an anti-phishing tool that protects the user against phishing websites that have been faked. The approach monitors sensitive information provided by users and generates alerts whenever such information is provided on the website.
2.	Thin Client [6]	A thin client is designed to ensure a secure connection between a client and the organization. This is really a healthier way of avoiding people losing their private or sensitive information because of phishing.
3.	PILFER [7]	To catch a large percentage of phishing emails, the tool can be deployed in a standalone configuration without a filtering system. It blends a collection of features with advanced machine learning approaches to capture fraud.
4.	An AntiPhishingApplication [8]	This tool established an end-user application that uses the data given by the user to validate the integrity of its URL of the destination and is therefore able to provide a more accurate prediction.

2. Scam

The influence of online interaction and email has decided to make everything too easy for blossoming email scams. These schemes often arrive by email, uninvited. The types of scams are, now coronavirus scams, banking scams, mobile scams, lottery scams and government grant Scams [4].

- **Coronavirus Scam:** Scammers may use misinformation and scare tactics to exploit individuals during the coronavirus (COVID-19) outbreak. They had the ability to reach anyone via phone, email, postal mail, text, or social media.
- **Banking Scam:** Banking scams comprise attempts to access the bank account. The most common banking scams are, overpayment scam, unsolicited cheque scam and automatic withdrawal.
- **Mobile Scam:** This scammer attempt to take someone’s personal information or money. Real-life phone calls, robocalls, and SMS messages can all be used to perpetrate scams. Callers frequently make misleading promises, such as offering opportunity to buy things, invest money, or receive free product trials. They can also make money available to people through free handouts and lotteries.
- **Lottery Scam:** Prize scammers try to use fake lotteries, sweepstakes, or other competitions to get money or personal information. Many of them say you won a reward but have to pay a fee to get it. Others allow you to enter a competition with personal details. Such scams

will reach people via postal mail, email, phone call, robocall, or text message.

- **Government Grant Scam:** Government grant scammers try to even get their money by guaranteeing people a cost subsidy such as university or home renovations. They ask for information about someone's checking account. They claim deposit the grant money into the account or deduct a "one-time processing fee" from it.

Table 2. List of tools to prevent the Scam

S.No	Tool Name	Description
1.	Geolocation [9]	When a customer places a new order, the geolocation technology recognizes the user virtual IP authentication server with the order. Likening the IP address of the device against all the on-file information with the issuer allows users to view that the buyer has submitted the request from a satisfactory destination.
2.	Proxy Piercing [9]	Geolocation can be tricked as offender's attempt to mask their IP addresses using proxies. This makes it more difficult to review both flag transactions based on the IP location, or monitor the location of a fraudster. One solution to cope with this hazard is through proxy piercing technology. Proxy piercing is intended to really see the user's actual identity through a proxy address and identify it.
3.	Device Fingerprinting [9]	Device fingerprint recognition is a forensic technique seen on the device used to identify every purchase made. The tool collects distinctive information on the installed operating systems on a device that is visiting the site. Each source of evidence helps to create a globally unique image, like human fingerprint lines.

3. *Phishing*

Phishing is a type of cybercrime in which someone impersonates a reputable organization in order to trick people into giving sensitive information such personal information, banking and credit card information, and passwords by email, phone, or text message. The data are then utilized to gain access to key accounts, potentially resulting in identity theft and financial loss. Legislation, user training, public awareness, and technical safety procedures are all possibilities for resolving phishing problems [4].

Table 3. List of tools to prevent the Phishing

S.No	Tool Name	Description
1.	Infosec IQ PhishSim [10]	Infosec IQ is more than just a phishing simulation model; together with its realistic phishing test results, it has new flexible training modules and customized programs that give the administrator ultimate control.
2.	Gophish [11]	Gophish is an open-source platform, which can be installed by simply downloading and retrieving a ZIP folder on most software applications. Characteristics are few but are implemented in a very impressive way. People can very easily build phishing template and while there is no one who comes along with the kit, there is a server from something that people can take support.
3.	King Phisher [12]	King Phisher is the open-source anti-phishing solution made by SecureState. It becomes one of the most advanced tools and it has some awesome features, like having phished users place, running several campaigns at once, and being able to do web cloning. Templates for both application Pages and messages are stored in the repositories.

4. *Identity Theft*

Identity theft is the criminal offense of acquiring another individual's personal or financial information for the purpose of considering the name or individuality of that person for the purpose of making transactions or sales. There are many different ways in which identity theft is committed. There are various types of identity theft which include medical, criminal, child and financial identity theft.

- **Medical**: In this theft, somebody designates himself as somebody else to be given healthcare for free.
- **Criminal**: A criminal mischaracterizes himself as just another person during the imprisonment to prefer to prevent a summons, to prevent a warrant issued in his real name from being discovered or to avoid a record of arrest or conviction.
- **Child**: Someone makes use of a child's identity for various types of personal enrichment.
- **Financial**: Somebody uses the identification or knowledge of another person to access to loans, products, services or privileges. This is perhaps the most prevalent form of identity theft.

Table 4. List of tools to prevent the Identity Theft

S.No	Tool Name	Description
1.	SolarWinds Identity Monitor [13]	With utmost diligence it monitors data for breaches, providing people with a secure and consistent solution. This is the best heritage monitoring device, because it is user-friendly, efficient and flexible.
2.	IdentityIQ [14]	It integrates credit agencies and score distribution, credit tracking, dark web tracking, identity security , application verification, restore identity, and family safety utilities to provide a range of security tools designed to alleviate the pressure.
3.	SoniqIdentityForce [14]	SoniqIdentityForce is an obvious contender and top-ranked tool, but it comes second because it's not as cost-effective as it might be.

		Nevertheless, it is indeed a realistic solution for security, authenticity, and mortgage security, with technological advancements for detection.
4.	LifeLock [15]	Norton-based LifeLock is a common option among people seeking robust identity monitoring services. The combination of Norton 360 with LifeLock gives you an all-in-one security solution that protects your privacy, your devices and your identity online. Through using Norton technology, this tool will block cyberattacks, which blocks an average of 142 million attacks a day. It also helps to block the public Wi-Fi details with a stable VPN and the system comes with antivirus software Norton, which is nobel prize-winning in the IT security field.

5. Spyware

Spyware is a kind of malicious programs or malware, which is assembled on a computer device even without knowledge of the individual user. It decides to invade the computer, steals private information and usage data on the internet, and relays it to retailers, data firms, or outside users. Any software that is downloaded without the user's permission may be categorized as spyware. Spyware became one of the most frequent threats against internet users. It monitors Internet activity once activated, records login credentials and spies on confidential information. Spyware's primary objective is typically to acquire credit card numbers, banking records, and passwords.

Table 5. List of tools to prevent the Spyware

S.No	Tool Name	Description
1.	Norton [15]	Norton is a global leader in combatting malware of all kinds — which include spyware. Even though Norton's antivirus engine uses artificial intelligence (AI), new and emerging threats are constantly being learnt. The malware scanner could detect 100% of the spyware
2.	McAfee’s security [16]	McAfee's security suite detects and removes spyware, viruses, and other malware across all platforms. It also comes with a slew of extra capabilities to protect you from spyware.
3.	TotalAV [17]	TotalAV offers really good anti-spyware protection and this product is used to detect the spyware with high capability.
4.	Bitdefender [18]	Bitdefender is a global leader in spyware detection and elimination, and all other malware forms.

IV. CONCLUSION AND FUTURE SCOPE

Online fraud comes in several ways. It ranges from viruses that target computers to retrieve personal information, to email systems that draw victims into connecting money. The strategies used by online fraud offenders are changing constantly. This paper reviewed the types of online or internet fraudulent and tools to prevent those attacks. Still, some of the threatening issues are existing in those tools. To overcome those issues, there is a need to develop new technologies and tools for preventing people from various types of online fraudulent.

REFERENCES

[1]. Hussein, Mohammed Juned, et al. "An evaluation of online proctoring tools." Open Praxis Vol.**12**, Issue.**4**, pp.**509-525, 2020.**

[2]. Wang, Shun-Yung Kevin, and Wilson Huang. "The evolutional view of the types of identity thefts and online frauds in the era of the Internet." Internet Journal of Criminology, Vol.**12**, pp.**1 - 21, 2011.**

[3]. Koong, Kai S., Lai C. Liu, and June Wei. "An examination of Internet fraud occurrences." pp.**441 – 449, 2012.**

[4]. Apte, Manoj, Girish Keshav Palshikar, and Sriram Baskaran. "Frauds in online social networks: A review." Social networks and surveillance for society, pp.**1–18, 2019.**

[5]. Chen, Juan, and Chuanxiong Guo. "Online detection and prevention of phishing attacks." 2006 First International Conference on Communications and Networking in China. IEEE, pp.**1-7, 2006.**

[6]. Lai, Albert M., and Jason Nieh. "On the performance of wide-area thin-client computing." ACM Transactions on Computer Systems (TOCS), Vol.**24**, Issue.**2**, pp.**175-209, 2006.**

[7]. Alkhalil, Zainab, et al. "Phishing attacks: A recent comprehensive study and a new anatomy." Frontiers in Computer Science, Vol.**3**, pp.**1-23, 2021.**

[8]. Varshney, Gaurav, Manoj Misra, and Pradeep K. Atrey. "A survey and classification of web phishing detection schemes." Security and Communication Networks, Vol.**9**, Issue.**18**, pp. **6266-6284, 2016.**

[9]. Srii Srinivasan, “A Merchant's Guide to Online Fraud Detection”, **2022.**

[10]. El Aassal, Ayman, and Rakesh Verma. "Spears Against Shields: Are Defenders Winning the Phishing War?" Proceedings of the ACM International Workshop on Security and Privacy Analytics, pp.**15 – 24, 2019.**

[11]. Ross, Philip E. "Microsoft to spammers: go phish [e-mail security]." IEEE Spectrum, Vol.**43**, Issue.**1**, pp.**48-49, 2006.**

[12]. Sonowal, Gunikhan. "Phishing Kits." Phishing and Communication Channels. Apress, Berkeley, CA, pp.**115-135, 2022.**

[13]. Martínez, Jeferson, and Javier M. Durán. "Software supply chain attacks, a threat to global cybersecurity: SolarWinds’ case study." International Journal of Safety and Security Engineering, Vol.**11**, Issue.**5**, pp.**537-545, 2021.**

[14]. Sahoo Anmol, Sahoo Aradhana, Prasad Srinivas, “ Enterprise Security Management(E-SRM)”, Indian Journals.com, Vol.**10**, Issue.**1**, **2012.**

[15]. do Produto, Manual. "Norton™ AntiVirus.", **2013.**

[16]. Kline, Jeffrey S. "McAfee Associates, Inc. Competitive Strategies for the Computer AntiVirus Industry."

[17]. Garba, Faisal A., et al. "Evaluating the state-of-the-art antivirus evasion tools on windows and android platform." 2019 2nd International Conference of the IEEE Nigeria Computer Chapter (NigeriaComputConf). IEEE, pp.**1-4, 2019.**

[18]. Pavel, Cosmin. "Bitdefender®, the award-winning provider of innovative antivirus solutions." Romanian Distribution Committee Magazine 4.1: **20-24, 2013.**