Research Article

A Critical Analysis of Fraud Cases on the Internet

Syed Anas Ansar[1], Jaya Yadav[2], Sujit Kumar Dwivedi*[3], Ankur Pandey[4], Savarni Prakash Srivastava[5], Mohammad Ishrat[6], Mohd Waris Khan[7], Dhirendra Pandey[8], Raees Ahmad Khan[9]

[1]BBA University, Department of Information Technology, Lucknow, India

[2]National Post Graduate College, Department of DDUKK, Lucknow, India

[3]BBA University, Department of Information Technology, Lucknow, India

[4]Bandhan Bank, Cluster Head, Lucknow, India

[5]Integral University, Department of Computer Application, Lucknow, India

[6]Integral University, Department of Computer Application, Lucknow, India

[7]Integral University, Department of Computer Application, Lucknow, India

[8]BBA University, Department of Information Technology, Lucknow, India

[9]BBA University, Department of Information Technology, Lucknow, India

[7]mwariskhan@iul.ac.in

Article History: Received: 11 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 23 May 2021

Abstract: We lived in the era of technology, where online websites have made communication and interaction much easier than the early decade. The modern world is changing so quickly, and emerging new trends simplify our lives, but on the other hand, it will also create risks. A website acts as a more admired platform by the user to access the different web applications. Because of the functions of the website, all the data on the website is available in the proper structure, which makes the working environment much convenient and efficient. The websites may undoubtedly be a precious resource for young people, but it may also cause severe problems. It is really easy to build a fake website that looks like an original website where hackers like to deceive consumers and businesses for their own benefits. In this paper, researchers have examined online fraud cases through web applications and how fraudulent websites affect financial loss. Researchers also highlighted the current situation regarding the usage of online services, as well as the threats that have an impact on users. In addition, researchers have suggested that new laws and regulations will be implemented for preventing cybercrime.

Keywords: Website, Security, Frauds, Financial Loss, Fraud Cases.

1. Introduction

We are surrounded by digital technologies, and it has made a significant contribution towards connectivity and knowledge sharing. The web has changed the way people do tasks dramatically. A website plays an enterprising role in the rapid evolution of information technology, and its industrial importance cannot be neglected. Unlike physical products, a website does not face wear and tear or deformity, but it can be corrupted, hacked, or damaged in numerous ways. A website will promote your work and business among consumers regardless of your company or profession and deliver strong messages whether your organization is a small, big, or well-established new brand.

Over the past few years, the Web has grown at an unprecedented pace. The number of internet users worldwide has doubled from 2009 to 2019 [1]. The user's internet browsing experience makes social websites more optimized for each user. Nowadays, many people surf different websites based on their uses [2]. A website will give you a platform to boost your work (i.e., working from home or any workplace), and through it, you can easily interact with anyone. The website has come of age and offers immeasurable endowment to many people's lives and we can access different kinds of facilities and more besides through websites [3]. Websites continue to grow at an unbelievable rate, with more data online than ever before. With the wide use of online transactions, exchanging information, internet surfing, data transfer etc., information technology resources are experiencing enormous growth [4]. It is very easy to build any website, and no one is going to judge whether this website is genuine or fraudulent. Most of the work is done online; a website acts as a future entrepreneur for an organization where people spend their time looking for the numerous services offered. Despite of these, it has also generated new threats, and it's a sad fact of life.

Today, there are more than 1.5 billion such websites on the World Wide Web fewer than 200 million of them are working. The peak of 1 billion websites is hit for the first time in September of 2014. As per a survey of internetlivestats, the overall number of sites has risen tremendously through 2016. The number of sites reached 900 million to 1.7 billion from January 2016 to December 2016 [5]. It is very simple to make a fake website that looks like an original website through which a "hacker" can access user's personal or bank details and even they can misuse." Online fraud is described as 'the experience of the person who responded to a fraudulent invitation, notification, offer or request through the web by providing personal detail or money, resulting in the suffering of a non-financial and financial loss or impact of some sort [6].

Unfortunately, some hackers create fake websites that aim to trick customers into sharing private information, such as their account numbers and credit cards. Scammers are fond of tricking customers and companies for their benefits; some hackers also make webpages that look close to Amazon and eBay. This raises a question about the status of website security. Consequently, the security of websites and other online software has become a battle, where a penetrator tries to find out loopholes and security experts try to patch them [7]. The main objective of this paper is to present the fraud report and identify the need for website security to protect individuals or organizational data.

The rest of the article has the following structure: the second section defines the related works, and in the third section, researchers address the related frauds. In section four major finding is discussed and finally, section 5 provides the conclusion.

2. Related Work

Researchers investigated how fraudsters took advantage of people and organizations for their gain. Several security mechanisms have since been established to shield networks and scammers from threats by individuals or

organizations. Some of the new researcher's works are analyzed in the field of fraud, online scams related to the website are discussed below:

Adam M. Bossler et al. (2020) address the online fraud victimization issue in which police departments face significant obstacles in responding adequately to incident reports. The main objective of this paper is to resolve the gaps in the understanding of the online fraud perceptions of constables and sergeants through a systematic review of survey data obtained from over 1300 officers from 35 local police departments across Wales and England. They examined the views of sergeants and constables about their readiness to respond to online fraud and identified factors that are significantly correlated with preparedness feelings in general. They highlighted the need for further constables training related to basic computer operations, basic information protection, and handling of digital forensic evidence. Improved familiarity with technology has been associated with improved preparedness feelings and confirms prior research. They suggest that the most likely way to enforce anti-fraud policies will be to influence police partners to make them aware of the nature of the issue and possible solutions [8].

Zhenzhen Nong and Sally Gainsbury (2019) have addressed social cues present in the online environment, which makes difficult for an individual to check their safety and recognize latent threats in online activities. This research will direct future studies to evaluate the effect of a website on online risk-taking behavior by identifying environmental indicators and potential social in website functionality and further contributing to online risk reduction [9]. In the same year, Alisdair et al., have published an article about how online scam is a big threat to cybercrime. The authors explain that the fraud occurred well before the internet came into existence and the most prevalent types of cybercrime radicalized on the internet. They illustrate it can be difficult to protect the offender's custody without a specific description of online fraud. The Directive must ensure the same basic framework for all countries within the Union. Therefore, the Directive must provide for a minimum standard of security across the Union. They must ensure a minimum standard of security for EU people for effectively tackling online fraud. There is a need to correlate the laws and set out a minimum framework to protect all online fraud victims from the most prevalent forms of online fraud [10].

Apapan and Liu (2018) introduced a deep learning auto-encoder (AE) and a restricted Boltzmann computer (RBM) to construct a model for detecting fraud in previous transactions. The proposed AE-based deep learning is an unsupervised learning algorithm that applies back propagation by setting inputs equal to outputs. The RBM has two layers, the (visible) input layer and the hidden layer. Additionally, they use three datasets; these are the German, Australian and European datasets. In this work, they use Google's TensorFlow library by using deep learning to implement AE, RBM, and H2O. They may infer from this research that AE and RBM produce high accuracy for larger datasets and AUC scores since there is a vast amount of data to be studied. They assured that the results of the European Dataset, AE, and RBM would make AUC (Area Under Curve) more reliable for the characteristics of the receiver operator than that achievable [11].

Krishna Modi (2017) has analyzed different types of fraud identification techniques. In this study, researchers addressed that the number of illegal transactions is growing rapidly. They also addressed the number of different approaches used to identify fraud cases, as well as fraud detecting issues. For detecting online fraud, banks and credit card companies use various data mining methods, i.e., Rule-based mining, decision tree, neural network, hidden Markov method, and either of these or a combination of these approaches may be used to detect online fraud. In addition, they may add new features and use different sampling methods to develop the algorithm more precisely. This paper aims to provide a comparative analysis of various techniques for detecting fraud [12].

In this paper, Cassandra Cross et al. (2016) have presented the analysis of in-depth interviews with a group of 80 people from across Australia who reported online fraud complaints involving losses of $10,000 or more over the previous years. This research was conducted to enhance the understanding of online fraud victims reporting experiences and their support needs by performing extensive interviews with a group of individuals who reported their victimization to the Scamwatch website of the ACCC. They also record their obstacles to reporting these incidents [13].

Roshan Jabee and M. Afshar Alam (2016) have addressed cybersecurity issues and threats of social networking sites. It is normal for social network users to share information, but they lose privacy when sharing information with strangers and fall into the honey trap they have created. However, several consumers are unaware of this and fall victim to breach of privacy and identity. So, they surveyed to find user views on the privacy and security of social websites and particular on Facebook, about the default privacy settings improvement. This research illustrates the need for enhancement of Facebook's default privacy setting to avoid cyber-attacks and publicly reveal personal details [14].

Mafaisu Chewae et al. (2015) have published a report in which they have mentioned that millions of internet users connected through online social networks in the era of advanced technology. They focused on how personal information is being affected by social networking websites. They also addressed how secrecy is vulnerability and how to minimize the loss of privacy risk. They highlighted the current situation about social network usage and the risks that could impact social networks [15].

Cassandra Cross and Dom Blackshaw (2014) have examined the response of police to online fraud. Police departments have historically given little consideration and priority to fraud, and this is heightened in the online world. This article highlighted Project Sunbird as an example of a proactive policy response aimed at victimizing online fraud in Western Australia. The West Australian Police (WAPOL) launched Operation Sunbird in May 2012 to investigate alleged movements of illicit funds between West African nations and West Australians. They discussed the numerous obstacles faced by police attempting to tackle online crime and explained how Project Sunbird's strategy seeks to achieve success by overcoming these obstacles. Ultimately, this paper explains that

the Sunbird project is a creative and strong base to enhance further the quality and efficacy of online fraud approaches [16].

Gangopdhyay and Dhar (2014) have highlighted the privacy issues in social networking sites. This report claims that social sites attract teenagers and provide them opportunities to get along with known & unknown persons. They mentioned several issues faced by the users, particularly teenage and young people are hacking, comment controversies, and identity theft. This paper discussed how social networking sites provide privacy protections and promote data sharing. Additionally, the paper would also examine the privacy settings of popular social media their effectiveness. In order for young people to be more cautious and aware, they must be aware of the advantages and drawbacks. SNS (Social Networking Sites) managers have to provide information on security risks and privacy issues. So, the virtual world is a safer place for all netizens, young and old alike, to work [17].

3. Related Fraud

The 21st century is the technological era in which new developments were made. The modern world is changing so rapidly that we can't keep track of all of its changes. Modern technology and new trends are being developed to simplify our lives [18]. We can share videos, images, music and can interact with each other through social sites and media from anywhere in the world. It has some advantages, but it also poses a series of challenges. Children and youth of today can easily be misled by the wrong content in some fake websites. Including various internet frauds such as illegal online purchases, bogus tech support schemes, and job scams are shown in table 1.

- COVID-19 Fraudulent websites: New typologies of fraud risk have already increased significantly, especially with regard to the registering of significant numbers of "COVID" internet domains. Such fake websites look like the organization's legitimate websites but are carrying the malware to attack computers or phone devices [19].

Table 1: Fraud Cases in the Last 11 Fiscal Years

Year	Cases	Amount (Crore)
2018-2019	6,800	71,500
2017-2018	5,916	41,167.03
2016-2017	5,076	23,933.85
2015-2016	4,639	18,698.82
2014-2015	4,639	19,455.07
2013-2014	4,306	10,170.81
2012-2013	4,235	8,590.86
2011-2012	4,534	4,501.15
2010-2011	4,093	3,815.76
2009-2010	4,669	1,998.94
2008-2009	4,372	1,860.09

- The Reserve Bank of India has said that over 6,800 cases of bank fraud involving an estimated Rs 71,500 crore were registered in 2018-19. Banks with Rs 2.05 Lakh crore have registered 53,334 fraud cases users in the last 11 fiscal years [20].
- On Feb 12, 2019, Manu Jain, Xiaomi India CEO has alerted the public to a new kind of fraud that is taking place using Xiaomi's name. In a tweet, Jain said that he had come across "a scam where few retailers have been cheated into buying a fake franchise of Xiaomi India Mi Stores!". He also mentioned that he saw forged documents with his fake signature [21].
- On Feb 06, 2020, a fake franchise issue of RealMe arose, where the fake website of RealMe offers partnerships to lure citizens [22].
- Online scams involve scammers claiming to be legitimate online vendors, either through fake websites or false ads on real retailers. The data used in this paper from the Australian Competition & Consumer Commission to aware consumers so they can report scams and get knowledge about such scams. These are certain online scam records [23].

3.1 Attempts to gain your personal information

There are several ways through which anyone can access your crucial data, i.e., Phishing, Hacking, Identity theft and Remote access scam, etc. In these, scammers use sly methods of all types to steal your personal information. If they have acquired this, they will use it to participate in illegal activities. The reports of such scams are shown in table 2 & 3 and the pictorial representation showed in figure 1 & 2, respectively [23].

Table 2: Fraud Cases to Gain Personal Information.

Months	**2017**	**2018**	**2019**	**2020**
Jan	3,629	3,763	5,032	4,500
Feb	4,689	4,198	4,926	5,101
Mar	4,764	4,396	4,381	4,083
Apr	4,948	4,416	3,690	6,309
May	6,072	5,148	4,104	4,127
Jun	6,145	4,851	3,499	5,686
Jul	4,460	5,478	5,065	7,056
Aug	4,727	4,564	4,825	8,164
Sep	4,686	4,246	4,357	10,532
Oct	4,719	4,828	5,379	10,023
Nov	4,464	6,142	5,079	8,808
Dec	3,228	5,030	3,544	7,810

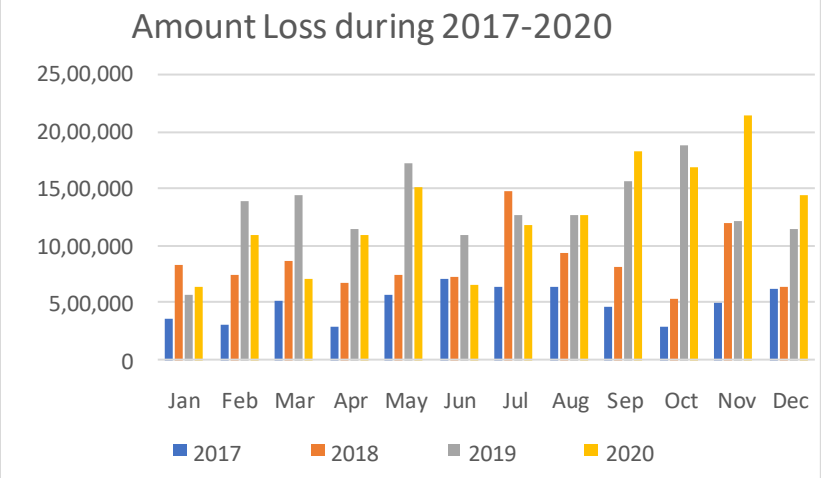

Figure 1: Amount Loss from 2017-2020

Table 3: Annual Fraud Report in the Last 4 Years.

Years	Amount Lost ($)	Number of Reports	Annual Financial Loses(percentage)
2017	5,977,877	56,531	2.8
2018	10,297,195	57,060	3.7
2019	15,805,156	53,881	4.2
2020	15,331,903	82,199	3.2

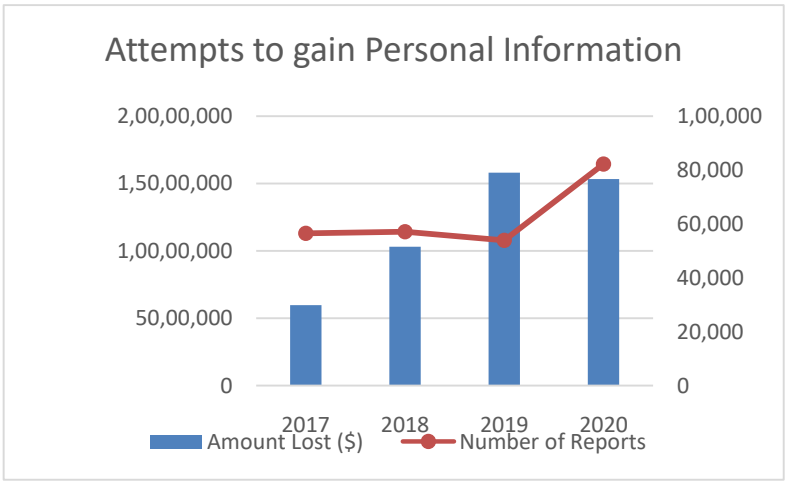

Figure 2: Annual Report of Financial Losses with Number of Reports

3.2Buying or Selling

Scammers are fond of tricking customers and companies that purchase or sell goods and services. Not all transactions are legal. Classified scams, False billings, Health and Medical products, Mobile premium services, Online shopping scams, Overpayment scams, Psychic and clairvoyant are some buying or selling frauds [23]. Details of this scam are shown from 2017- 2020 in table 4 and 5. The pictorial representation are showed in figure 3 & 4 respectively.

Table 4: Fraud Cases of Buying or Selling.

Months	**2017**	**2018**	**2019**	**2020**
Jan	2,856	2,827	2,886	2,978
Feb	3,653	2,929	2,797	3,334
Mar	2,864	3,442	2,582	2,784
Apr	2,469	2,491	2,337	3,243
May	3,621	2,740	2,404	3,118
Jun	3,687	2,800	2,102	3,167
Jul	2,808	2,368	2,656	3,490
Aug	3,090	2,637	2,584	3,604
Sep	3,146	2,348	2,408	3,793
Oct	4,434	2,970	2,761	3,660
Nov	3,112	2,785	2,879	4,046
Dec	2,827	2,846	2,728	4,000

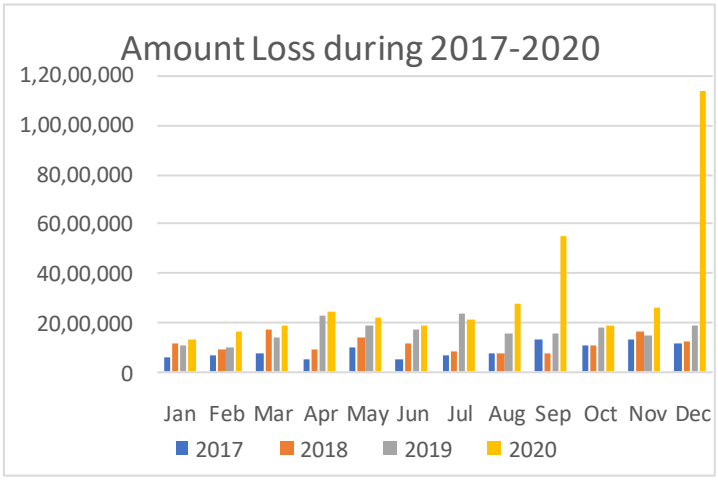

Figure 3: Amount Loss from 2017-2020

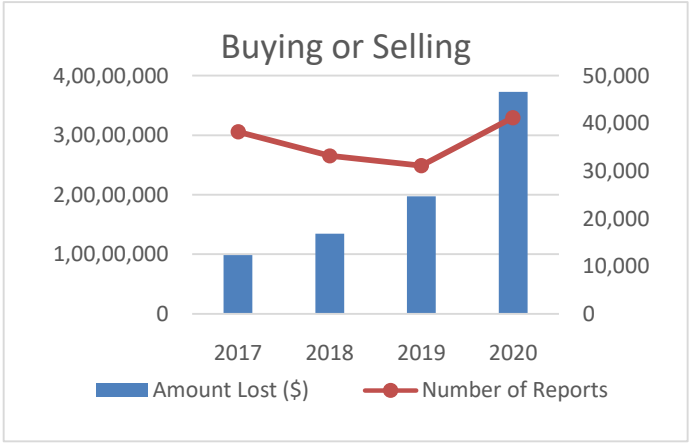

Figure 4: Annual Report of Financial Losses with Number of Reports

Table 5: Annual Fraud Report in the Last 4 Years

Years	**Amount Lost ($)**	**Number of Reports**	**Financial Loses(percentage)**

2017	9,842,632	38,236	21.1
2018	13,437,420	33,183	28.7
2019	19,708,392	31,119	33.4
2020	37,286,902	41,217	33.5

3.3Online Shopping Scam Records

A recent online shopping scam version includes social media sites to set up fake online stores. For a limited time, they open the shop, often selling fake branded clothes or jewellery. The shops are closing after having made a lot of sales. They even use social media to promote their fake website, just because you've seen it promoted or posted on social media [23].

- Vinay Malik (name changed) IT specialist, ordered a mobile from the top e-commerce platform. Upon the arrival of the product, it had a stone in the box. Malik is not the only one. There are several instances in which buyers did not get the products they requested, and then e-tailer duped them [24].
- As of March 2017, evidence reveals online retail fraud cases have arisen almost six times. With just 977 instances of this kind of fraud between August 2016 and March 2017, the figure more than doubled to 2,441 for the 2017 to 2018 financial year. This dramatic growth persisted in the financial year 2019 with a rise of more than 100 percent as shown in figure 5.

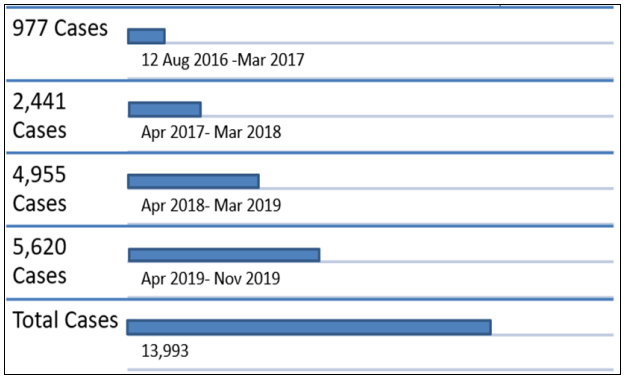

Figure 5: Online Retail Fraud Cases

According to the latest reply from Lok Sabha by Piyush Goyal, Minister of Commerce and Industry, in the first eight months of the financial year 2020, the number of frauds reported under the e- portal at the National Consumer Helpline increased further to 5,620, increasing the total to 13,993 as of August 2016 [24].

Below is the list of scam records from 2017 to 2020 as shown in table 6 and 7. Their pictorial representations are shown in figure 6 and 7 respectively.

Table 6: Fraud Cases of Online Shopping.

Months	**2017**	**2018**	**2019**	**2020**
Jan	502	734	915	1,062
Feb	528	523	725	1,083
Mar	533	524	767	945
Apr	459	784	749	1,224
May	690	908	778	1,191

Jun	586	976	657	1,237
Jul	481	848	805	1,419
Aug	507	1,007	790	1,443
Sep	611	817	803	1,407
Oct	564	748	865	1,337
Nov	751	863	992	1,512
Dec	591	959	1,107	1,447

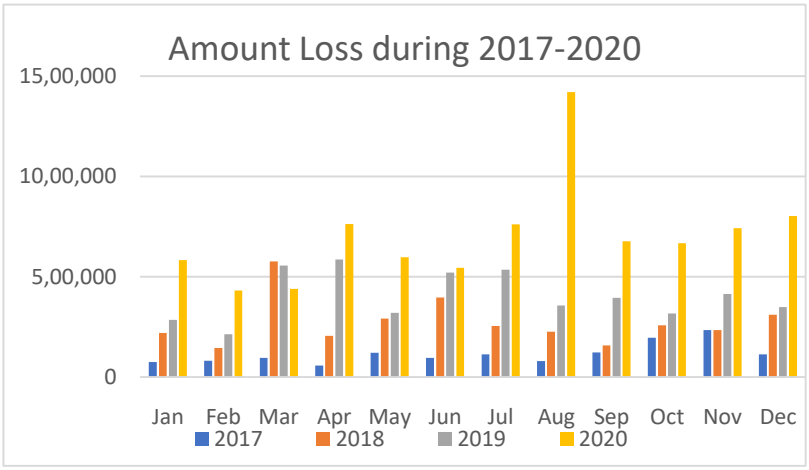

Figure 6: Amount Loss from 2017-2020

Figure 7: Annual Report of Financial Losses with Number of Reports

Table 7: Annual Fraud Report in the Last 4 Years.

Years	**Amount Lost ($)**	**Number of Reports**	**Financial Loses(percentage)**
2017	1,380,563	6,803	48.8
2018	3,278,776	9,691	57.3
2019	4,845,452	9,953	60.6
2020	8,428,525	15,307	55.1

3.4Jobs and Employment scam

Scammers identify as career advisors and approach the chairman of institutes or colleges directly. They offer positions in large and respected businesses, then bill a lump amount. They usually vanish before carrying out the planned interviews. In this scam, they offer you a guaranteed job with a highly payable salary by manipulating you. See below for detailed reports of these scams from 2017-2020 as shown in table 8 and 9. Their pictorial representations are shown in figure 8 and 9 respectively [23].

Table 8: Fraud Cases of Jobs and Employment.

Months	**2017**	**2018**	**2019**	**2020**
Jan	226	210	310	185
Feb	262	250	265	196
Mar	276	254	299	225
Apr	201	248	434	384
May	273	287	241	311
Jun	314	291	210	278
Jul	251	207	277	323
Aug	227	272	207	341
Sep	199	280	235	265
Oct	272	354	235	265
Nov	216	254	213	303
Dec	175	258	174	268

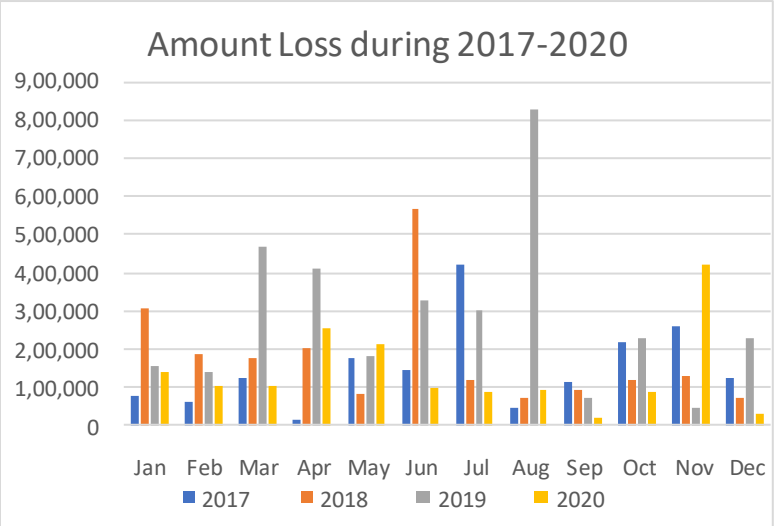

Figure 8: Amount Loss from 2017-2020

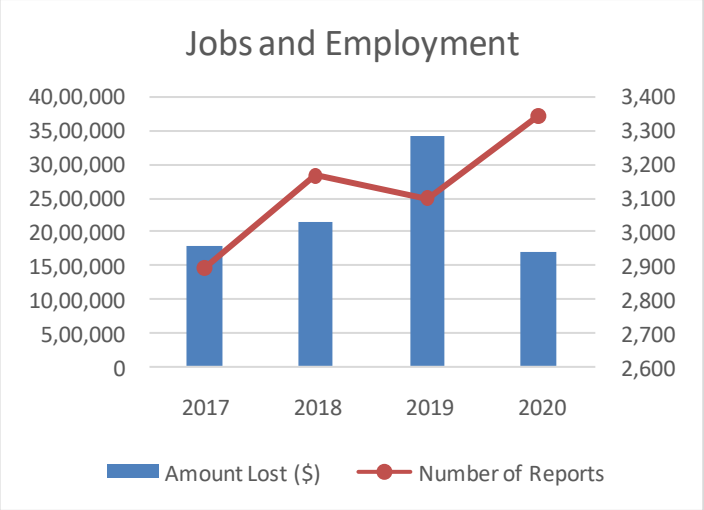

Figure 9: Annual Report of Financial Losses with Number of Reports

Table 9: Annual Fraud Report in The Last 4 Years.

Years	Amount Lost ($)	Number of Reports	Financial Loses(percentage)
2017	1,792,180	2,892	8.1
2018	2,132,198	3,165	13.6
2019	3,396,999	3,100	19.5
2020	1,674,308	3,344	11.6

3.5Fake Charities

Scammers set up a website that looks like legitimate charities websites and seeks donations or emails you pretending to raise money after major disasters or diseases. Below is the list of scam records from 2017 to 2020 as shown in table 10 and 11. Their pictorial representations are shown in figure 10 and 11 respectively [23].

Table 10: Fraud Cases of Fake Charities.

Months	2017	2018	2019	2020
Jan	90	67	86	408
Feb	102	93	109	108
Mar	121	92	97	156
Apr	80	60	67	155
May	110	75	119	90
Jun	121	85	81	79
Jul	93	69	117	84
Aug	106	80	103	86
Sep	83	68	87	70
Oct	81	80	94	57
Nov	89	86	102	57
Dec	69	86	105	77

Table 11: Annual Fraud Report in the Last 4 Years.

Years	Amount Lost	Number of	Financial

	($)	Reports	Loses(percentage)
2017	313,563	1,146	10.6
2018	211,165	941	13.6
2019	411,588	1,167	14.1
2020	218,214	1,427	12.2

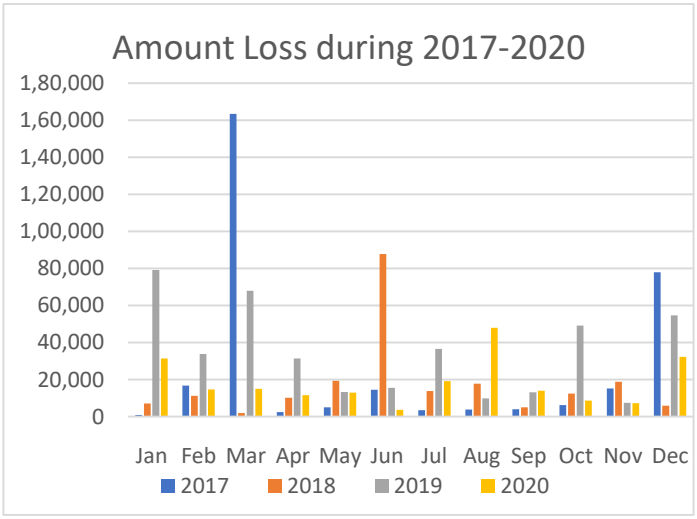

Figure 10: Amount Loss from 2017-2020

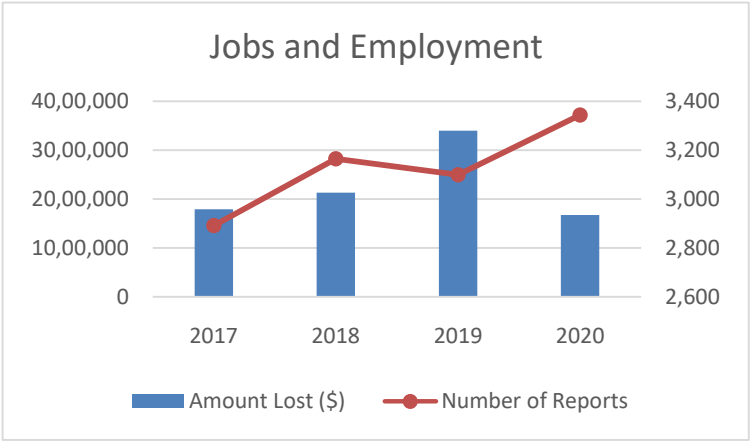

Figure 11: Annual Report of Financial Losses with Number of Reports

3.6Threats and Extortion

Scammers can use every means at their fingertips to steal your money or identity -including accessing your confidential information and hijacking your device. They can easily threaten you with malware and ransomware attacks and threats to life, arrest, or another way. These Scams statistics are given below from 2017 to 2020 as shown in table 12 and 13. Their pictorial representations are shown in figure 12 and 13 respectively [23].

Table 12: Fraud Cases of Threats and Extortion.

Months	2017	2018	2019	2020
Jan	507	554	5,403	397
Feb	926	584	2,248	405
Mar	783	687	1,465	418
Apr	422	480	1,103	3,600

May	683	444	886	918
Jun	526	683	969	2,492
Jul	1,437	1,686	1,716	3,353
Aug	1,690	1,178	1,185	3,800
Sep	2,075	1,892	1,073	6,763
Oct	1,938	2,381	856	6,936
Nov	1,109	7,211	580	3,999
Dec	613	6,031	402	3,005

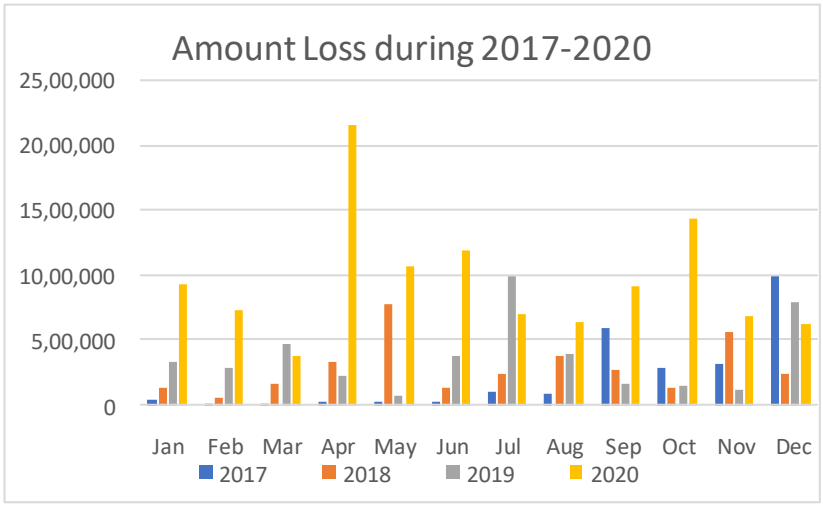

Figure 12: Amount Loss from 2017-2020

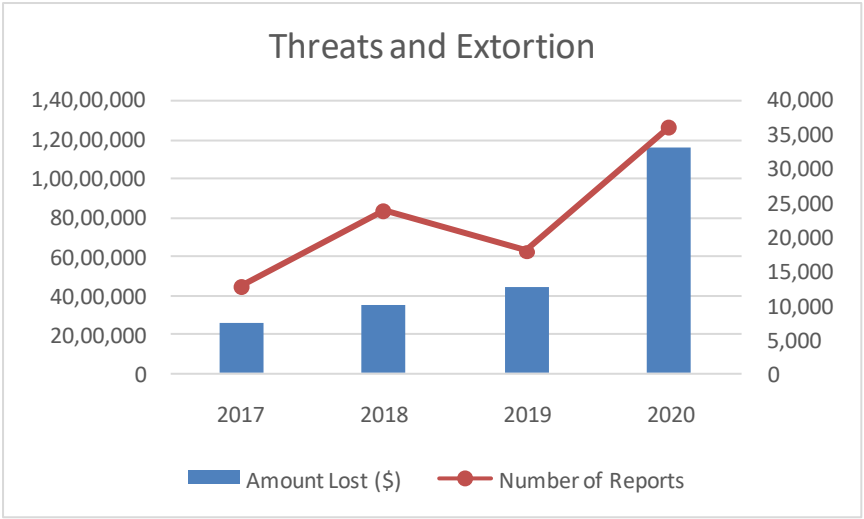

Figure 13: Annual Report of Financial Losses with Number of Reports

Table 13: Annual Fraud Report in the Last 4 Years.

Years	**Amount Lost ($)**	**Number of Reports**	**Financial Loses(percentage)**
2017	2,539,912	12,709	2.8
2018	3,490,181	23,811	1.8
201	4,411,958	17,886	2.6

9			
2020	11,520,460	36,086	2.4

3.7Investments

The scammer seeks a way to obtain entrance into such a community or group and provides the target audience investing options for safe returns. What he has to do to succeed is persuade the leader or an important member.

- More than $26 million was documented lost to investment fraud in 2018 - 84 percent of the overall losses registered in 2017 already. This reflects an annual month-over-month rise of 117 percent in damages relative to the previous year [25].
- From 2017 to 2020, financial losses were rapid increases [23].

Below is the list of fraud cases of investments from 2017 to 2020 as shown in table 14 and 15. Their pictorial representations are shown in figure 14 and 15 respectively.

Table 14: Fraud Cases of Investments.

Months	**2017**	**2018**	**2019**	**2020**
Jan	514	521	313	430
Feb	673	595	460	549
Mar	788	723	435	539
Apr	603	366	507	647
May	859	455	510	552
Jun	833	352	496	610
Jul	630	285	721	751
Aug	642	309	504	843
Sep	880	299	391	877
Oct	755	329	400	734
Nov	717	366	411	569
Dec	482	264	360	671

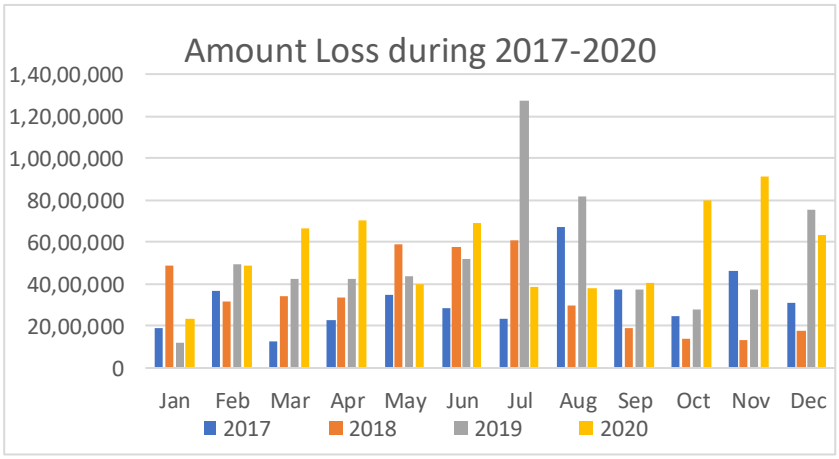

Figure 14: Amount Loss from 2017-2020

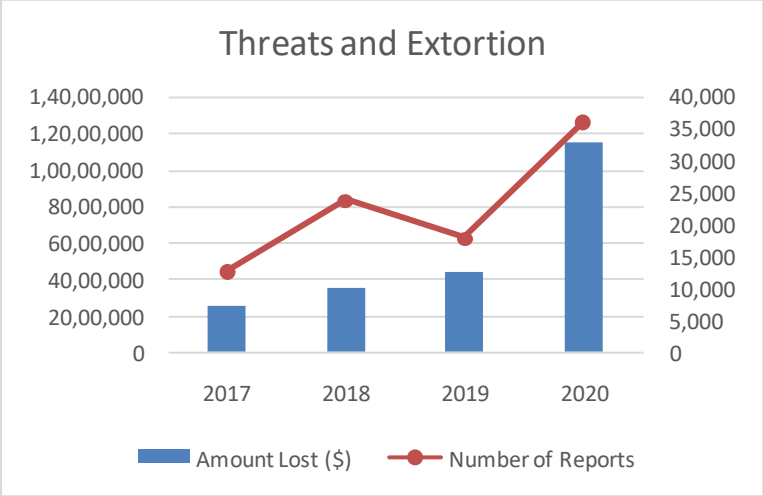

Figure 15: Annual Report of Financial Losses with Number of Reports

Table 15: Annual Fraud Report in The Last 4 Years.

Years	Amount Lost ($)	Number of Reports	Financial Loses(percentage)
2017	38,348,457	8,376	12.8
2018	41,966,415	4,864	27.6
2019	63,018,402	5,508	41.0
2020	67,081,314	7,772	35.3

3.8Unexpected Money

This scam is similar to Nigerian Scams. In, Nigerian scams someone from abroad who offers you a share of a large sum of money on helping them move money from their country. Although these scams have arisen in Nigeria, they are now coming from around the world. Inheritance scams, Rebate scams, and Nigerian scams record from 2017 to 2020 as shown in table 16 and 17. Their pictorial representations are shown in figure 16 and 17 respectively [23].

Table 16: Fraud Cases of Unexpected Money.

Months	2017	2018	2019	2020
Jan	1,852	1,189	549	420
Feb	2,074	1,240	469	366
Mar	1,877	1,550	561	289
Apr	1,683	574	442	434
May	2,173	746	513	268
Jun	2,359	645	385	354
Jul	1,967	565	571	387
Aug	1,977	480	373	318
Sep	1,541	482	340	338
Oct	2,037	388	366	304
Nov	1,563	755	308	259
Dec	975	407	224	332

Figure 16: Amount Loss from 2017-2020

Figure 17: Annual Report of Financial Losses with Number of Reports

Table 17: Annual Fraud Report in The Last 4 Years.

Years	Amount Lost ($)	Number of Reports	Financial Loses(percentage)
2017	9,279,270	22,078	6.4
2018	4,772,468	9,021	6.8
2019	3,911,841	5,102	5.2
2020	2,808,903	4,069	6.1

3.9Dating and Romance

In a very short time, dating and romance scammers will show strong feelings towards you and recommend you move the relationship. They will ask you (subtly or directly) for your banking or credit card details, gifts or money until they have won your confidence and your resistance are down. They will even ask you to give yourself photographs or videos. From 2017 to 2020, financial losses were rapid increases as shown in table 18 and 19. Their pictorial representations are shown in figure 18 and 19 respectively [23].

Figure 18: Fraud Cases of Dating and Romance.

Months	2017	2018	2019	2020

Jan	348	341	352	376
Feb	320	334	340	397
Mar	338	315	331	300
Apr	267	278	319	313
May	331	338	333	301
Jun	248	310	277	340
Jul	323	314	339	346
Aug	354	330	377	275
Sep	306	341	327	273
Oct	360	317	307	266
Nov	324	431	341	247
Dec	244	332	305	238

Figure 18: Amount Loss from 2017-2020

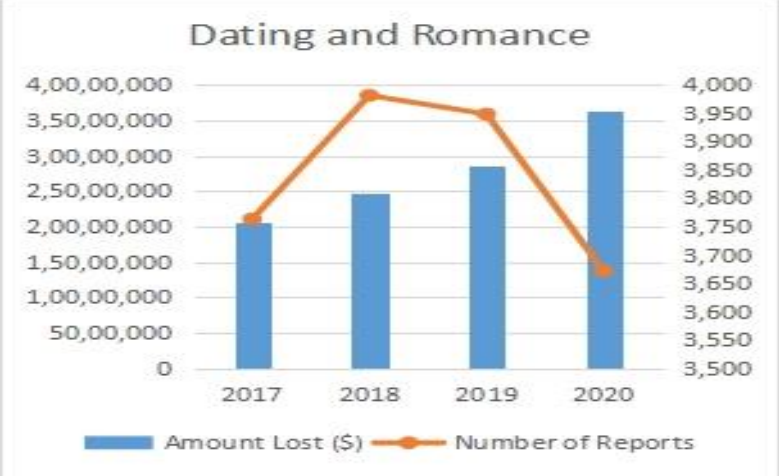

Figure 19: Annual Report of Financial Losses with Number of Reports

Table 19: Annual Fraud Report in The Last 4 Years.

Years	**Amount Lost ($)**	**Number of Reports**	**Financial Loses(percentage)**
2017	20,530,578	3,763	23.5

2018	24,648,024	3,981	30.8
2019	28,606,215	3,948	35.0
2020	36,217,859	3,672	35.4

3.10Unexpected Winnings

Scammers ask you to pay some amount of fees to win your prize or claim it. Scratchier scams, Travel prize scams, Unexpected prizes, and lottery, these scammers make fool users gain their profit. These Scams statistics are given below from 2017 to 2020 as shown in table 20 and 21. Their pictorial representations are shown in figure 20 and 21 respectively [23].

Table 20: Fraud Cases of Unexpected Winnings.

Months	**2017**	**2018**	**2019**	**2020**
Jan	1,023	1,347	628	425
Feb	931	1,113	770	400
Mar	1,176	1,151	1,023	257
Apr	1,031	1,005	836	281
May	1,205	985	803	256
Jun	1,057	1,065	664	216
Jul	1,107	880	1,603	271
Aug	1,925	1,121	1,817	462
Sep	1,394	885	1,074	379
Oct	1,546	793	655	425
Nov	2,212	936	565	652
Dec	1,187	790	506	813

Table 21: Annual Fraud Report in the Last 4 Years.

Years	**Amount Lost ($)**	**Number of Reports**	**Financial Loses (percentage)**
2017	2,176,938	15,794	2.3
2018	3,368,510	12,071	3.5
2019	3,165,156	10,945	5.0
2020	1,980,788	4,837	7.8

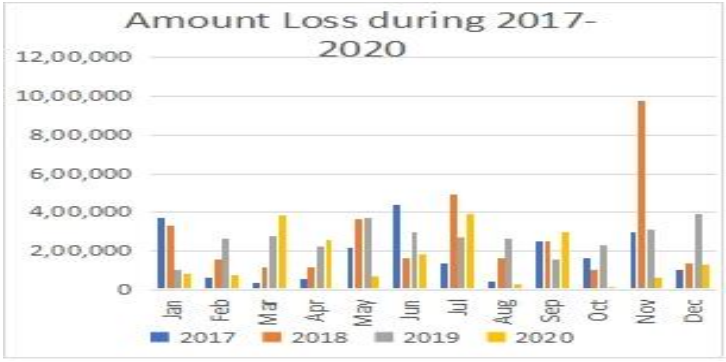

Figure 20: Amount Loss from 2017-2020

Figure 21: Annual Report of Financial Losses with Number of Reports

3.11Online Scam Records of last 4 years

The list of online scams in different sectors is shown in table 22.

Table 22: Several Severe Fraud Reports in the Last 4 Years.

Online Scam	Amount Lost ($)	Number of Reports	Financial Loses(percentage)
Online Shopping Scam	17,933,316	41,754	221.80
Unexpected Winnings	10,691,392	43,647	18.60
Investments	210,414,588	26,520	116.70
Dating & Romance	110,002,676	15,364	124.70
Jobs & Employment	8,995,685	12,501	52.80

4. Major Findings

Websites have greatly changed the way people accomplish a certain task, like finding information and communicating with each other through social media using the internet. The complexity of the online world makes it very hard for individuals to recognize threats, check their safety and take adequate precautions. Several results collected during the study are discussed below:

While fraud has been practiced throughout history, the Internet's emergence has created new and innovative ways to target potential victims.

- Web fraud presents a big problem for society as regards the monetary losses and the debilitating effects on the victims.
- These days, social sites are one of the simplest ways of interaction and have become an inevitable phenomenon for the young. Since these sites are becoming increasingly common, they serve as a tool for cybercrime and attacks.
- As the number of these cashless transactions, online jobs, and online shopping rises, fraudulent transactions also grow.
- Victim support services are focused mainly on victims who have experienced violent crime rather than financial damage. This lack of assistance can also heighten the risk of being a victim of online fraud.
- A provision must be made to protect the victim's privacy so that the victim can complain about their online fraud complaint to the police.
- There is no fast-rapid court to deal with cases of online scams. There is a need for a different cell, where the issue relating to fraud is resolved, and citizens get justice

5. Conclusion and Future Scope

We lived in the era of technology, where websites have made communication and interaction much easier than the early decade. In this paper, researchers have highlighted the complexity of the online world and provide a detailed fraudulent record in all most every category of online scams, which makes it very hard for youth to recognize it. Websites keep on rising at an unprecedented pace, with more data online than ever before. Building any website is very simple, and nobody can judge whether this website is genuine or fraudulent. Users are using the website in increasing numbers, progressively every day. It is easier to build a website than you would imagine. The design of a website and application makes the creation and transmission of messages almost easier for an organization. Anyone can build a website and can add a payment gateway with verification, and no one is questioning the authentication and reliability of payment in these websites. Now the whole world is suffering from COVID-19, but apart from that, there are various COVID-19 fraud cases that have occurred, where scammers claim that government departments need personal information with the help of text messages and 'phishing' emails. These include malicious links and attachments intended to steal your personal and financial data. Fake websites also attempt to imitate legal corporate domain names. Researchers also highlighted the present situation with regard to the usage of online resources and the risks that can impact users. To overcome from these, a new framework must be introduced to check the authenticity of these websites and new laws and regulations should be enforced. At the same time, for such a problem a new court should be formed because

there is no quick-fast trial court. So, there is a need for separate cells to take action related to online scams so that the citizens get justice. Researchers are developing a new framework for the prevention, identification, and remedies against online fraud to prevent these problems in the future to solve this problem. Besides this, there is still a lot of research work needed on privacy and protection to create secure web applications.

References

1. Online Available at: https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/
2. Bansal, Chetan & Bhargavan, Karthikeyan & Maffeis, Sergio. (2012). Discovering Concrete Attacks on Website Authorization by Formal Analysis. Journal of Computer Security. 22. 247-262. 10.1109/CSF.2012.27.
3. Renaud, Karen. (2006). A Visual-Biometric Authentication Mechanism for Older Users. 10.1007/1-84628-249-7_11.
4. Ansar, Syed & Kumar, Satish & Khan, Waris & Khan, Prof. Raees. (2020). Enhancement of Two-Tier ATM Security Mechanism: Towards Providing a Real-Time Solution for Network Issues. International Journal of Advanced Computer Science and Applications. 11. 123-130. 10.14569/IJACSA.2020.0110717
5. Online Available at: https://www.internetlivestats.com/total-number-of-websites/
6. Cross, Cassandra & Smith, R.G. & Richards, K.. (2014). Challenges of responding to online fraud victimization in Australia. Trends and Issues in Crime and Criminal Justice.
7. Ansar, Syed & Agrawal, Alka & Khan, Prof. Raees. (2018). A Phase-wise Review of Software Security Metrics. 10.1007/978-981-10-4600-1_2.
8. Bossler, Adam & Holt, Thomas & Cross, Cassandra & Burruss, George. (2020). Policing fraud in England and Wales: examining constables' and sergeants' online fraud preparedness. Security Journal. 33. 10.1057/s41284-019-00187-5.
9. Nong, Zhenzhen & Gainsbury, Sally. (2019). Website design features: Exploring how social cues present in the online environment may impact risk taking. Human Behavior and Emerging Technologies. 2. 10.1002/hbe2.136.
10. Gillespie, Alisdair & Magor, Samantha. (2019). Tackling online fraud. ERA Forum. 20. 10.1007/s12027-019-00580-y.
11. Pumsirirat, Apapan & Yan, Liu. (2018). Credit Card Fraud Detection using Deep Learning based on Auto-Encoder and Restricted Boltzmann Machine. International Journal of Advanced Computer Science and Applications. 9. 10.14569/IJACSA.2018.090103.
12. Modi, Krishna. (2017). Review on fraud detection methods in credit card transactions. 10.1109/I2C2.2017.8321781.
13. Cross, Cassandra & Richards, K. & Smith, R.G.. (2016). The reporting experiences and support needs of victims of online fraud.
14. Jabee, Roshan & Afshar, M.. (2016). Issues and Challenges of Cyber Security for Social Networking Sites (Facebook). International Journal of Computer Applications. 144. 36-40. 10.5120/ijca2016910174.

15. Chewae M., Hayikader S., Hasan M H. and Ibrahim J. 2015 How Much Privacy We Still Have on Social Network? International Journal of Scientific and Research Publications, Volume 5, Issue 1, January 2015 Edition, page no:1.
16. Cross, Cassandra & Blackshaw, Dom. (2014). Improving the Police Response to Online Fraud. Policing. 9. 119-128. 10.1093/police/pau044.
17. Gangopadhyay S and Dhar M. D. social networking sites and privacy issues concerning youths. Article – 2 Global Media Journal-Indian Edition Sponsored by the University of Calcutta/www.caluniv.ac.in ISSN 2249 – 5835 Summer Issue/June 2014/Vol. 5/No. 1.
18. Online Available at: https://medium.com/@gpccio/21-century-is-the-era-of-technology-4956d5c86671.
19. Online Available at: https://assets.kpmg/content/dam/kpmg/in/pdf/2020/03/forensic-covid-19-frauds-and-scams.pdf.
20. Online Available at: https://economictimes.indiatimes.com/news/economy/finance/bank-fraud-touches-unprecedented-rs-71500-crore-in-2018-19-rbi/articleshow/69631871.cms.
21. Online Available at: https://www.indiatoday.in/technology/news/story/some-people-are-now-trying-to-open-fake-xiaomi-india-stores-and-scamming-people-1454037-2019-02-12.
22. Online Available at: https://timesofindia.indiatimes.com/gadgets-news/realme-issues-a-public-warning /article show/73986482.cms
23. Online Available at: https://www.scamwatch.gov.au/about-scamwatch/scam-statistics.
24. Online Available at: https://www.businesstoday.in/current/economy-politics/online-shopping-frauds-jump-6-fold-in-over-2-years/story/391975.html.
25. Online Available at: https://www.scamwatch.gov.au/news/beware-investment-wolves-knocking-at-the-door.