Fraud in Online Classified Ads: Strategies, Risks, and Detection Methods: A Survey

Article *in* Journal of Applied Security Research · September 2022

DOI: 10.1080/19361610.2022.2124328

3 authors, including:

Jamil R. Alzghoul

3 PUBLICATIONS **11** CITATIONS

SEE PROFILE

Emad E. Abdallah

Hashemite University

55 PUBLICATIONS **732** CITATIONS

SEE PROFILE

Routledge
Taylor & Francis Group

Journal of Applied Security Research

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/wasr20

Fraud in Online Classified Ads: Strategies, Risks, and Detection Methods: A Survey

Jamil R. Alzghoul, Emad E. Abdallah & Abdel-hafiz S. Al-khawaldeh

To cite this article: Jamil R. Alzghoul, Emad E. Abdallah & Abdel-hafiz S. Al-khawaldeh (2022): Fraud in Online Classified Ads: Strategies, Risks, and Detection Methods: A Survey, Journal of Applied Security Research, DOI: 10.1080/19361610.2022.2124328

To link to this article: https://doi.org/10.1080/19361610.2022.2124328

JOURNAL OF APPLIED SECURITY RESEARCH
https://doi.org/10.1080/19361610.2022.2124328

Fraud in Online Classified Ads: Strategies, Risks, and Detection Methods: A Survey

Jamil R. Alzghoul[a], Emad E. Abdallah[b], and Abdel-hafiz S. Al-khawaldeh[c]

[a]Cyber Security and Information Technology Department, Jordan Armed Forces, Amman, Jordan; [b]Department of Information Technology, Faculty of Prince Al-Hussein Bin Abdullah II for Information Technology, The Hashemite University, Zarqa, Jordan; [c]University Education Department, Jordan Armed Forces, Amman, Jordan

ABSTRACT

Because of today's tremendous economic growth, social, and technological advances, the world has seen the formation of economic blocs. The intensity of the rivalry between domestic and foreign products has increased to improve their capacity in terms of quality and price, while e-commerce has grown in popularity, both with exhibitors and consumers. The citizens can search the internet for their needs at any time, in any country, but new risks have emerged that threaten the consumer who purchases and concludes contracts electronically, such as fraud risks, misrepresentation, commercial extortion, and piracy, as well as the consumer's inability to truly inspect the contractual object, and so on. In this survey, we give a study that clarifies the types of deceptive ads that are made online, whether through spam or popular advertising sites like Craigslist or online dating, and we show what action may be taken to prevent ad fraud.

KEYWORDS

Deceptive ads; electronic fraud; commercial extortion; piracy; fake advertisements

Introduction

The rapid advancement of technology has increased the importance of computers in many areas of modern life; there is no longer a branch of any activity that does not use a computer in its transactions, including but not limited to banks, companies, bodies, airports, sales, purchase, leasing, and others. The computer's importance originates primarily from the programs and systems it employs in its operations. It is the mind that governs the computer because it is the only way to organize, store, and display information in an orderly manner, not to mention the INTERNET, which contains a wealth of important information and through which many services and legal processes, such as buying and selling, leasing, and electronic payment, are carried out, as the World Wide Web brings the entire world within reach.

CONTACT Jamil R. Alzghoul Jamilalzghoul@gmail.com Cyber Security and Information Technology Department, Jordan Armed Forces, Amman, Jordan

This article has been corrected with minor changes. These changes do not impact the academic content of the article.

Nowadays, with the widespread use of the Internet in all parts of the world, and the tremendous increase in the processes of buying, selling, and renting through the Internet, a large number of people are using websites to carry out purchases and sales to save time and effort, as well as to get a better deal, because E-marketing is done through free ads (Chaffey & Smith, 2013), and by using the consumer's home computer, it allows for continuous follow-up and monitoring, but Ease of falling prey to some untrustworthy sites, whose goal is fraud and theft after the transaction is completed, as well as the likelihood of incompatibility of the genuine product features with the bogus features that these fake sites boast about.

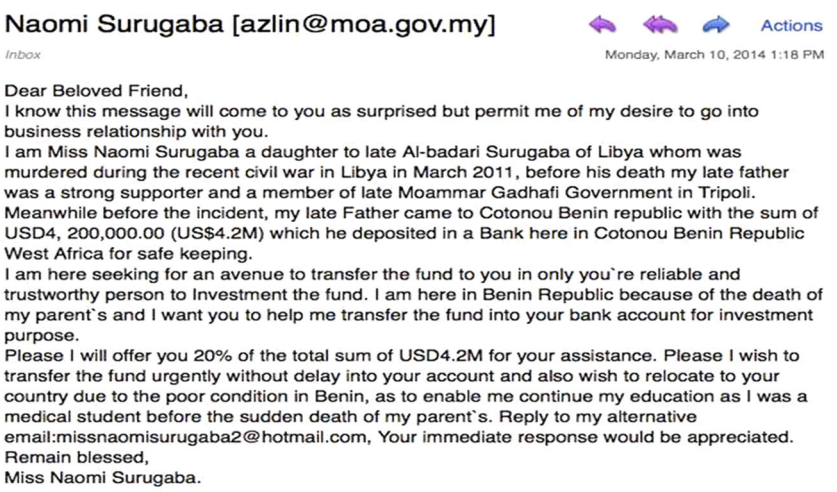
Due to the closure to the outbreak of the Corona epidemic, there have been many applications, websites, and electronic sales offers these days, in addition to the long closure period has made us in need of many it includes products from food, clothing, electronic devices, furniture, books, and many other products.

There are also fraudulent websites that offer readers to sign up for a paid mailing list with a monthly fee to receive advance information about pre-foreclosure properties. All of these factors necessitate the use of online shopping, so we must proceed with caution and ensure that we know exactly what we want to buy to avoid being victims of fraud.

This astounding growth of commercial transactions from buying and selling via the Internet has resulted in the emergence of crimes resulting from that use, and these crimes either occur on the computer itself, or it occurs utilizing the computer where it becomes a tool in the hands of the perpetrator who uses it to achieve his criminal purposes, or what is referred to as electronic crime, which is a crime carried out using a computer via an internet connection. Deviant behavior, with its material and moral pillars, constitutes a crime, and it does not cross the line with the motivation to commit it.

With the spread of the internet throughout the world, it has become more difficult to monitor and expose these crimes since they cross borders, have no control over them, and are carried out at great speed without supervision, account, or oversight from any country. This resulted in the commission of all forms of criminal activity recognized on the Internet, such as robbery of computer programs to steal data and even the secret information database and its use in espionage, or those related to piracy and money robbery, as well as the emergence of what has been termed electronic terrorism and threatening the national security of countries.

Prostitution of children and women is used, whether by eye or minors, by photographing them directly or by simulation and digital representation of the image, using means of incitement and intimidation, such as seduction, warning, or threat, as well as crimes of public morals and ethics


Naomi Surugaba [azlin@moa.gov.my]

Actions

Inbox

Monday, March 10, 2014 1:18 PM

Dear Beloved Friend,
I know this message will come to you as surprised but permit me of my desire to go into business relationship with you.
I am Miss Naomi Surugaba a daughter to late Al-badari Surugaba of Libya whom was murdered during the recent civil war in Libya in March 2011, before his death my late father was a strong supporter and a member of late Moammar Gadhafi Government in Tripoli.
Meanwhile before the incident, my late Father came to Cotonou Benin republic with the sum of USD4, 200,000.00 (US$4.2M) which he deposited in a Bank here in Cotonou Benin Republic West Africa for safe keeping.
I am here seeking for an avenue to transfer the fund to you in only you`re reliable and trustworthy person to Investment the fund. I am here in Benin Republic because of the death of my parent`s and I want you to help me transfer the fund into your bank account for investment purpose.
Please I will offer you 20% of the total sum of USD4.2M for your assistance. Please I wish to transfer the fund urgently without delay into your account and also wish to relocate to your country due to the poor condition in Benin, as to enable me continue my education as I was a medical student before the sudden death of my parent`s. Reply to my alternative email:missnaomisurugaba2@hotmail.com, Your immediate response would be appreciated.
Remain blessed,
Miss Naomi Surugaba.

Figure 1. Example of advance fee fraud.

through electronic pornography embodied by pornographic sites, especially directed including children under the age of puberty.

All theories and studies agree on one fundamental point: the purely material goal that the cyber-criminal seeks to achieve, in particular, electronic fraud operations ranging from the robbery of funds to the assault on confidential data and the destruction of information programs for any country to threaten its national security and territorial integrity.

Cybercrime is distinguished by its transnational nature, with perpetrators in one location and victims in another, as well as the speed with which it is carried out, as well as the destruction of evidence and the erasure of its effects, not to mention the fact that it is committed by extraordinary people with superintelligence and high technology in dealing with information technology and computers.

Frauds have become quite popular; here are some real-life examples of frauds that occurred with people on Craigslist and other sites. The first example (Beware of craigslist rental scams, 2021) is an apartment rental fraud offered on Craigslist in two different areas of Maryland. This is an example of two Craigslist ads that are identical. It could be promoted on other websites. First, it is listed on Craigslist Baltimore: $435 Bright and Spacious 2 Bedroom 2 Bath unit rent in Baltimore (Baltimore). It is once again listed on Craigslist Frederick: Rent a bright and spacious 2-bedroom 2 bath unit in Frederick for $435 per month (Frederick).

In a different case of advance fee fraud, the victim receives an email from the fraudster asking him to help him retrieve his money in exchange for a large quantity of money (The most common examples of a phishing email, 2021). To complete the process, the fraudster asks the victim to provide his banking details, such as account number and so on (see Figure 1).

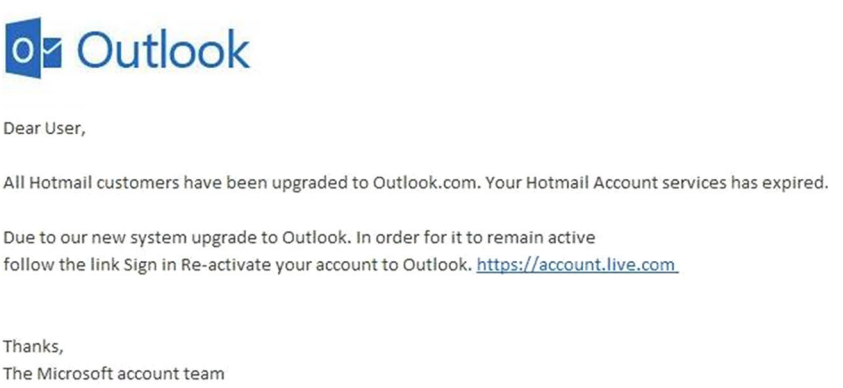


Figure 2. Example of email upgrade fraud.

In The most common examples of a phishing email (2021) shows an example of an email upgrade fraud. You will be prompted to update your e-mail address, as it will expire if you do not do so. The e-mail appears to be from a reputable source, such as Google or your employer's IT department. A link appears in the e-mail. If you click on it, you will be taken to a website where you will be asked for personal information or your account will be stolen. Alternatively, you can obtain your password. An example of email upgrade fraud is shown in Figure 2.

Credit card fraud and information theft are shown in Online Card Fraud - FraudSMART (2021). Martina's credit card was used without her knowledge in a vending machine. Martina received a letter from her bank requesting that she contact them. She called the bank to find out that her credit card had been used without her permission. Her card had been used for 686 euros on a well-known selling website. Martina was astounded that she had never used the site and that it was so simple to get her credit card information.

The techniques used to investigate fake advertisements are compared and analyzed in this survey. The rest of the paper is organized as follows: in Section "Problem statement & definition," we discuss the problem statement and definition, as well as communication channels. In Section "The most typical methods of ad fraud," we discuss the most common techniques of advertising fraud and the symptoms of internet advertising fraud. Section "Fraudster's techniques" discusses Fraudster's techniques. Section "Background studies" presents background studies, while Section "Discussions & research directions" contains research directions. Finally, bring the survey to a close by offering suggestions for future projects.

Problem statement and definition

The risks to which the electronic consumer is exposed include: The hazards of electronic shopping are numerous and diverse, with various

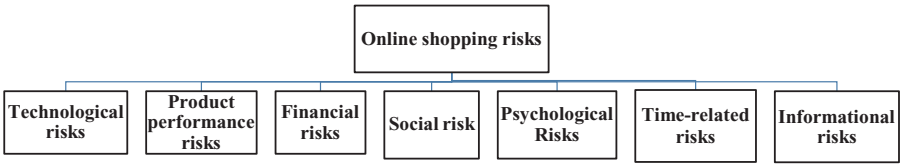


Figure 3. Types of online shopping risks.

ramifications for consumer behavior in online shopping, and they are difficult to manage. E-commerce technology is continually changing and developing, and with each change or development comes a new set of threats. Consumer behavior researchers have discovered various sorts of risks that customers experience when purchasing online, including functional, physical, social, temporal, and financial concerns. For internet customers, these threats are viewed as possible risks that prevent them from purchasing. Figure 3 depicts the risks in detail.

A more extensive breakdown of these concerns is provided below:

- Technological risks: risks that may arise from consumer use of technology, such as the device being vandalized due to viruses and the lack of physical communication in the purchase, as well as information loss due to the Internet, which may be cut off in the middle of the application process, or even if the buyer is exposed to a technical obstacle (Andrews & Boyle, 2008).
- Product performance risks: This is the risk that the product will not perform as expected, and it refers to the state of the consumer's fear that the product will not match the expected benefits, as well as the agreed specifications and quality, which is the loss that the buyer can bear if the product does not perform as expected. To the utmost extent possible, he must fulfill what is required of him (Brown et al., 2007; Pi & Sangruang, 2011).
- Financial risks: These are risks that have financial effects for the consumer, such as the fear that the product is not worth the price paid for it, or the fear of losing the money spent to receive the commodity due to fraud (Arshad et al., 2015; Brown et al., 2007).
- Social risk: It refers to the worry that making the wrong product decision would cause consumer discomfort or make him the target of ridicule; for example, to buy online and making an unwise online purchase (Forsythe & Shi, 2003).
- Psychological Risks: Consumers may acquire psychological difficulties, loss of trust in dealing or shopping over the Internet, and psychological frustration because of exposure to commercial fraud and fraud through the Internet. Consumers will be disappointed (Arshad et al., 2015; Forsythe & Shi, 2003).

- Time-related risks: This refers to the time spent purchasing a product online as well as the time lost because of a poor decision. This reflects the consumer's anxiety of wasting time looking for the thing they want to buy, as well as the chance that no fraud is suspected (Arshad et al., 2015).
- Informational risks: These are information security risks, and they include the risks of making decisions based on misleading, inaccurate, or inappropriate information obtained through fraud or obtaining information from a victim for later use against him, as well as the fraudulent use of websites and pages communication and profiles (Arshad et al., 2015; Järveläinen, 2007).

In this survey, we will be able to identify and comprehend the most common types of fraud and be aware of the deception channels and strategies used by fraudsters. Moreover, we will determine the monetary value of internet fraud and how it affects people's behavior. Finally, we should be able to recognize and comprehend the clues that can be used to detect internet-advertising fraud perpetrated by fraudsters.

Communication channels

The most prevalent means of communication via which people are subjected to deceptive or fraudulent actions. Those who were victims of frauds were most likely to have been victimized by e-mail, phone, and online advertisements (Flasy, 2020) as shown in Table 1. Email is the most common channel for scams and fraud, with online advertisements coming in third, far ahead of other channels like SMS/text messaging or postal letters. Nonetheless, phone calls continue to be a significant channel for scams and fraud, and the results clearly show that scams and fraud are not primarily limited to online behavior, but are also frequently carried out by phone (whether it be mobile or landline).

The most typical methods of ad fraud

Advertising designers attempt to be creative in their campaign design and implementation, much as fraudsters can be clever and efficient in their

Table 1. Online communication channels were the most frequently used for scams and fraud.

Communication Channels	Percentage
1. E-mail	(43%).
2. Phone	(28–15% by their mobile phone 14% by their landline phone).
3. Online advertisements	(11–7% on a "non-social media" website and 5% on social media, a blog, or forum).

branding fraud schemes. Here are the most common ad fraud tactics, ranging from domain spoofing:

1. Domain spoofing: The fraudster benefits from domain spoofing by convincing the advertiser that he is paying for a higher type of position, the quality of the traffic, and the content of the website, as the higher the position for the higher the quality in return, the publisher can charge a higher amount and consist of the following mechanisms (Amarasekara et al., 2020; Bashir & Robertson, 2017). URL substitution: By replacing the original URL with a bogus one, advertising might offer quotes for additional space.
   Cross-domain embedding: this entails using two websites, one with high traffic but low-quality inventory and the other with low traffic but high-quality inventory. In this case, the fraudster employs an iframe to overlay the higher-quality site on top of the low quality, high-trafficked one.
   Custom browsers: Robots can visit any website and change the URL to look like the URL of a different site.
   Human browsers: similar to traditional malware, when a visitor's system becomes infected and visits other websites, the malware will take over and use an ad placement.
2. Cookie stuffing: Cookies are stolen and erroneous information is provided for the visitor, and the marketer receives credit by selling, converting, or clicking (Amarasekara & Mathrani, 2016; Singla, 2018).
3. Click injection: A method by which a fraudster might boost revenue by creating phony clicks in an advertisement scenario, where these clicks frequently move to an advertisement or download an application, hence increasing revenue dramatically (Minastireanu et al., 2019).
4. Click spamming: A method of increasing money by creating illegal clicks on spam, however, it is less effective than Click injection (Dave et al., 2013).
5. Pixel stuffing: Instead of displaying a huge number of advertisings in an 11-pixel region, fraudsters place a massive advertisement in a spot that is too small to be detected (Dörnyei, 2021; Suresh et al., 2019).
6. Ad stacking: It converts a single ad spot into many ad locations, so the visitor can view one ad but it is placed on top of other advertising (Dash & Pal, 2020).
7. Ad injection: Ad injection is the process of creating clicks when none previously existed. Ads can be injected in the same way. Ad injection allows fraudsters to place advertising where they do not belong by using browser extensions and adware plugins (Dave et al., 2013).
8. Geo masking: The cost of creation varies depending on location since a certain geographical place is targeted and the focus is on it if clients from this location are likely to produce more value (McCormick & Eberle, 2013; Springborn & Media, 2013).

Table 2. The commonly used fraud signs from fraudsters and their implications.

Scam signs	Indications of use
VOIP contact phone number	Difficult to identify and discover
Frequently use common deceptive words	Such as overseas military personnel, outside the country, uncommon errors in grammar or idiom usage
Payment methods and transactions that cannot be tracked and verified	PayPal, MoneyGram, bitcoin, Western Union
Ad images	Unreal photos
Same Ad, multiple posting, same location	Intensify the publication of the advertisement
Determine the physical address of the advertiser	Misleading consumers or convincing them of the legitimacy of advertising, especially rental ads
The service/item cost	The price is illogical or alluring

Scam signs in online ads

The most common signs of online fraud that can assist consumers in determining the legitimacy of the advertisement, and these notifications can be used by researchers and developers in building automated detection systems that determine the legitimacy of these ads, although some of these signs do not necessarily evidence that the advertisement is fraudulent, but it increases the possibility of advertising fraud, informs the consumer, and raises awareness. Table 2 outlines the most typical fraud indications employed by scammers and their implications

- VOIP contact phone number: Scammers utilized it since it is difficult to track and modify (Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020; Park et al., 2014).
- Quite frequently Use common deceptive terms: where fraudsters use certain words in their statement to convince consumers of the announcement's credibility (Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020).
- Untraceable payment methods and transactions: Fraudsters employ untraceable payment methods such as PayPal, MoneyGram, bitcoin, and Western Union (Park et al. 2017).
- Ad images: Fraudsters use photographs discovered in advertisements or elsewhere to advertise when they do not own the ad or when the goods are in poor shape (Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020).
- Same ad, several postings, same location: to allow fraudsters to reach the greatest number of people possible (Lee et al., 2021).
- Determine the advertiser's physical address: This is especially important in advertising linked to renting and property, as it is used to persuade customers of the validity of the advertisement (Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020).
- The service/item cost is too good to be true: when the price of the product displayed in the advertisement is lower than the typical price, it

attracts more customers and indicates the possibility of fraud (Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020).

Fraudster's techniques

Fraudsters use various techniques to trap victims and obtain money in fraudulent ads. Many studies Al-rousan, Abuhussein, Alsubaei, Collen, et al. (2020) and Hu et al. (2011) have previously been conducted to research the fraud that is carried out on classifieds ads sites via the internet, which is intended to deceive consumers into revealing sensitive information and sending money. Some of this research concentrated on detecting fraud in classified advertising for sale, purchase, and rent published by well-known websites such as Craigslist, Amazon, and others.

Other studies concentrated on detecting fraud in job advertisements (Vidros et al., 2017) because it has a significant influence on the reputation of institutions, as well as the breach of applicants' privacy, in addition to financial losses.

Romantic fraud on the internet (Buchanan & Whitty, 2014; Whitty, 2013) is one of the most common operations, particularly in the West, and it is one of the collective marketing frauds. Previous research has been conducted to determine what romantic fraud is via the internet due to its financial, psychological, and other risks to people.

Some advertisements are produced by spam, which is regarded as a commercial enterprise to generate significant revenue through unsolicited mail. Some research (Huang et al., 2018; Perera et al., 2013; Rastogi et al., 2016) has been undertaken to better comprehend, evaluate, and battle spam. Phone fraud operations are one of the most common types of fraud carried out these days, owing to the widespread usage of smartphones by people of all ages, as well as their significant impact on saving time, effort, and money. Advertisements are aired and communicated via the Internet or through fictitious user numbers, fooling them into installing needless apps by seductive and terrifying graphics or phrases, resulting in significant financial losses.

Technical support scams (Miramirkhani et al., 2016, 2017) are attempts by fraudsters to persuade victims that their machines are contaminated with malicious or defective programs. Furthermore, they persuade people that they require technical support by allowing them to remotely access their equipment, invading the privacy of ordinary users, and demanding significant quantities of money to acquire support, which is essentially a procedural fraud.

419 Nigerian messages known as (advance fraud fee), which is one of the types of fraud perpetrated through fraudsters' emails to induce the victim

to transfer money to them (Castro, 2013; Smith & Holmes, 1999). They utilized empathy, confidence, and an unconvincing appeal to greed to afflict the victim and grab their money.

Click fraud is one of the types of internet fraud that occurs by hiring people and their guests to click on advertising content or deceiving consumers with adverts to boost clicks and make money (Almeida & Gondim, 2019; Zhu et al., n.d.).

Message fraud refers to fraudulent operations carried out via phone messages or chats. To safeguard consumers from fraud, studies have been performed to examine the content of these communications in order to construct systems and educate consumers about the ways that fraudsters employ this technology. Previous research focused on websites participating in survey fraud survey services in order to disclose the social engineering methods employed by online fraudsters, in which users are referred to other sites and requested to fill out a questionnaire in order to acquire a specific service (Jane et al., 2012; Shaari & Ahmed, 2020).

Background studies

The detection of misleading advertisements that are widely disseminated on websites, especially well-known websites like Craigslist and Amazon, has been the subject of numerous studies. We will discuss earlier research in this area that was done using techniques for identifying fake advertisements in this section.

Studies using conventional detection techniques

Alan McCormick and William Eberle (2013) did another investigation. Traditional data mining methods and machine learning algorithms (Nave Bayes, Multilayer Perceptron's (artificial neural network), J48, decision trees, and random forests) are used to extract associated features from an online classified advertising database. This method was used to find the links between fraudulent activities; numerous features were retrieved from existing attribute data. The data employed in the WEKA tool, however, had a limited number of features.

In Kharraz et al. (2018) describes a machine learning strategy for automatically identifying survey scams. The technology was used to identify websites involved in scam survey services, and the results were used to demonstrate that end users are exposed to identity theft, fraud, bogus programs, and malware. To create the detection model, information is gathered from the website's content, traffic, and general page display. They made use of elements such as suggestive graphics, user input forms,

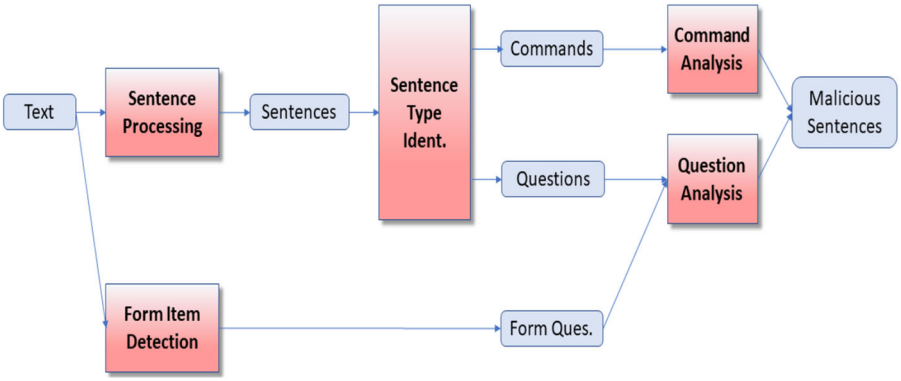


Figure 4. The process of text analysis based on command and question sentences.

third-party scripts, word sequences, web content, third-party answers, and image size. The study produced good results in detecting fraudulent surveys, but there are some limits in using it because the program is based on supervised learning, which means that attackers can change their website design strategy to escape detection. Furthermore, the authors did not rely on the tools employed by attackers to analyze IP addresses and keywords.

In Kim et al. (2019), a tool named Scam Detection Assistant (SDA) is introduced. The SDA examines attack content to detect social engineering attacks, and they employ semantic analysis to grasp the fundamental features of communication meaning. It is based on asking questions of the attackers in order to determine whether the responses to those questions had unique meanings or necessitated a banned operation. Figure 4 depicts the process of analyzing the text based on the command and questions sentences that are relevant to the study. They analyzed the text using the pars tree. However, the study requires an automated tool to analyze the text using deep learning algorithms to extract the feature set and determine the frauds in the text; additionally, new features such as IP address, phone number, and shipping address must be investigated.

To detect online fraud, a classical machine learning (logistic regression) approach was utilized in Sharifi et al. (2011), as well as a supervised machine learning approach. They employed internet advertisements and emails, as well as an offline resource, to collect data for studies. They studied 200 spam messages to identify various sorts of online fraud, including prepayment and phishing, medical fraud, and fraudulent dating, among others. They produced five datasets of authentic and phishing websites, which are as follows: (Scam queries, Web of Trust, Spam emails, hp Hosts, and Top websites). They employed ten-fold cross-validation on each dataset to test the devised technique, and the results were 98% in recognizing fraud informally. However, this system is only used as a Google Chrome browser

extension, which requires more data to be more accurate, and alternative algorithms can be applied to larger data sets.

In Vidros et al. (2017), the authors described the use of information and text-based classification to predict job frauds on the Internet. To perform the study, they constructed an equal set of data consisting of 450 authentic employment announcements and 450 false employment announcements. They also deleted all unexpected non-English words, as well as the normal English stop words. They used the Wikka tool, implementing six algorithms to classify the data, transform it into vectors, and then compare the findings. In the experiments, the random forest classifier was utilized. Pay attention to user behavior, company and network data, and IP and user content collision patterns.

Levchenko et al. (2011) did another study in which the authors concentrated on three types of advertising in spam: pharmaceuticals, software, and replicas. They gathered URLs from spam emails and stored them in a massive multi-terabyte (Postgres) database. They used the DNS crawler to identify the name server framework used to augment spam promoted spaces, as well as the address records used to host those names. They collected the complete domain name and domain suffix from each URL, and the crawler then does a recursive query on these spaces. It distinguishes between successful and definitive spaces, and it filters out unregistered domains and spaces with inaccessible title servers. They use content clustering to link sites with similar lexically content structures in order to classify them separately.

Automatic detection methods

Convolutional Neural networks (CNN) and Deep Neural networks (DNN) are used to create a smart system in Huang et al. (2018). They collected 150,000 advertising from daily ads and discovered that applications and porn sites are the most common sources of false ads. Experiment results have shown success in spotting fraudulent marketing on cell phones. They must, however, minimize the complexity of the jobs and continue the studies with large amounts of data.

In Miramirkhani et al. (2017), the authors present a study on bogus technical support messages. It is accomplished by identifying deceptive and erroneous advertisements, which are the primary cause of technical support victims, as through these deceptive advertisements they built an automated system called ROBOVIC, which works weekly for eight months to detect the ranges and phone numbers managed by fraudsters. Initially, they established a dependable system for identifying and collecting technical help fraud pages from prominent websites. The data was then evaluated to learn about the technologies used by technical support fraudsters, namely the

domains, phone numbers, and scam page contents, to determine the common terms used by scammers. The next held 60 meetings with technical support fraudsters, giving them access to virtual equipment, before analyzing the social engineering tactics and tools used by fraudsters and lastly educating and guiding customers about technical support scams. However, the attacker can adjust his strategy so that he is not detected by ROBOVIC. During the training phase, a supervised machine-learning-based classifier must be used.

In another study, Li et al. (2012) investigated harmful advertising and associated infrastructure. They spent three months scanning 90,000 websites. And did an intensive investigation to understand fraudulent advertising activities, using the prominent aspects of harmful ads and associated content distribution pathways to design a new system called MadTracer that detects fraudulent advertisements by constructing an autonomous detection foundation.

They focus on display ads and thoroughly examine dangerous ads identified from safe browsing by Microsoft, Google, and Forefront. They do a detailed analysis of harmful advertising reported from safe browsing in order to expose the cloaking techniques used by the malicious ad, URL, and domains. To identify publishers and advertising nodes linked to an unrelated to the publisher, they studied three primary entities: the node, path, and domain path. The MadTracer system has been demonstrated to be successful against malicious ad activity, detecting 15 times as many bad domain pathways as Microsoft Forefront and Google Safe Browsing combined, and it has also detected another sort of assault known as click-fraud attacks. However, we can see from the study that the other elements, aside from the triple nodes on which it is built, are not included in this study, and attackers may also change the patterns of the URL addresses.

The click fraud in internet advertising was presented in Minastireanu et al. (2019). The authors concentrated on detecting click fraud in online advertising, therefore they used a collection of data available on Kaggle, which deals with 200 million clicks in four days. In this work, the LightGBM algorithm was employed to sort and categorize operations. They used a variety of single and combination dataset attributes such as device, OS, IP, and app). To assess the classifier's accuracy, the data was separated into k-fold equal sections. The leaf-wise tree growth algorithm is used in the algorithm. They ran numerous tests, and the results were superior to and faster than the XGBoost method. Due to a lack of resources for training with all data sets, the study requires improvement.

Suarez-Tangil et al. (2020) did another study in which they built a method that depends on a deep neural network for early automatic detection (machine learning) of romantic scammers in bogus dating accounts.

The report includes the fraudsters' images and policies, as well as their demographics and the characteristics of the victims they fabricated.

A large database containing 14,720 fake dating files and 5,402 random samples of real files was created to understand and analyze the differences between these two types of files by combining image analysis mechanisms with advanced text categorization based on text analysis in dating files using LWIS. They employed several attributes collected from the text and photographs in the dating data, including age, gender, and description terms. They employed the Naive Bayes and Random Forests classifiers to classify demographic information, and the SVM classifier to identify photos. They trained each classifier on the training set features separately and in combination. The study got good accuracy results in detecting fraudulent dating files, but it did not apply to dating files on other sites, and the study also requires the use of additional elements to reach high accuracy.

Al-rousan, Abuhussein, Alsubaei, Kahveci, et al. (2020) conducted a study to detect and identify fraudsters in online dating, where many fraudsters utilize celebrity photos to attract attention. A technology called social guard was created to identify celebrities in bogus online dating accounts and classify them as false. The social-guard has done this by utilizing the AWS Rekognition and Google Vision APIs. AWS Rekognition analyzes suspicious profile photographs and determines whether they belong to celebrities. If so, it names the celebrity and provides a percentage confidence level. Google Vision searches the internet for suspicious photos and URLs that are partially or entirely matching images to assist users in determining the veracity of the profile. The technology has been shown to be capable of locating celebrity photographs.

In a study undertaken by Al-rousan, Abuhussein, Alsubaei, Collen, et al. (2020), the authors propose a program with intelligent components that automatically detects the likelihood of fraud in commercial adverts, specifically on the Craigslist site. Three frequent scams have been identified as red flags: (1) using ad graphics that already exist at other online Uniform Resource Locators (URLs), (2) using a VoIP phone number as a contact number, and (3) employing typical scam keywords in advertisements. To detect the risk of scam adverts, a web-scraping Python package, Google Vision, and Google Storage are utilized.

Another study on Craigslist users is proposed in Park et al. (2014), and they conduct this study on Craigslist users. The writers concentrated on bogus payments (Nigerian). They placed magnetic honeypot advertising to attract fraudsters and drive out honest users in order to better comprehend the fraudulent Nigerian on Craigslist. They examined the emails they received and reacted to as a result of their advertisements. An automated system is designed to acquire data by disseminating advertisements and

collecting fraudulent e-mails in order to engage with the fraudsters. To locate the fraudsters, the IP addresses of the scammers are collected, and the observations of the scammers are divided into groups depending on essential parameters such as phone number, shipping address, email address, and IPs.

The most common method of fraud is the receipt of a fraudulent PayPal notice saying that funds have been transferred to the victim's PayPal account, after the victim's request to send the product to the bogus address. They classified emails into groups based on internal similarity in their characteristics, such as if a chain of fraud uses the same phone number, email address, and shipping addresses, it is classified as the same group of scammers and discovered more than ten groups that account for roughly half of all fraud attempts. They discovered, however, that the used shipping address and IP are situated in Nigeria and America, thus they were unable to pinpoint the actual location of the cargo and had no idea where the stolen products were sold.

Studies carried out utilizing manual research detection techniques

In Park et al. (2017), the authors offer an experimental preliminary investigation of property rental scams on Craigslist. The authors classed fraudulent rental advertising based on two criteria: first, the ad is not available or does not belong to the advertiser. Second, misleading those who are interested in advertising by charging them in advance. The study depended on following up with the Craigslist rental department in different geographical places to collect the ad lists that were published in this area and then investigating the ads that were classed as fraudulent.

To plan phony postings into fraud campaigns, a manual search for fraudulent rental advertising and human-created standard articulations is used. A limited number of advertisement lists were discovered that they were unable to distinguish as real or fake. A specific conversation engine is designed that automatically connects with the publisher to verify the advertisement's legitimacy (gathering information by talking to fraudsters). They then checked five other major websites for advertising that had been reposted on Craigslist by fraudsters. They observed that 5 of the 7 main fraudulent operations were carried out with credit cards in 141 days, and 29,000 fraud announcements were spotted in 20 monitored cities using the payment methods utilized to check the frauds.

Sofo et al. (2010) examined the content of fraudulent emails to determine the psychological indications and methods most typically employed in frauds to alert consumers to illicit transactions, as well as to investigate the potential relationship between online abuse and consumer thinking. They

used three e-mail accounts to do their investigation, two from the same university and one from a commercial company. To filter spam, all of these accounts apply security guidelines. However, the study only looked at a few samples (three accounts only). Relationships were not examined using statistical analysis or the real application of consumers' thinking skills based on their replies to unsolicited e-mail.

In Button et al. (2014) conducts an accurate and in-depth interview with victims of fraud, six focus groups, and nine individual stakeholders involved in the battle against fraud. The interviews focused on the style of the deception, the effects, and the sort of injury. The study suggested certain fraud prevention strategies, such as warning and educating consumers about the dangers of fraud. However, the study did not consider the electronic methods that fraudsters employ in internet-based fraud operations, and there are no unique traits that can be used to classify the legality of the fraudulent activities.

In Alsaleh and Zhou (2018), 81,505 mobile phone advertising from Craigslist are collected. Inferential techniques are used in experiments and data analysis to discover fake advertisements. The advertising was either current or expired, or they had been flagged as fake by the same site. They sorted and organized the data before beginning to examine the marked Craigslist ads. The price was one of the inference strategies they employed, as a price that is too high or too low is proof of fraud. Identify the highlighted craigslist ad as a scam and compare it to another comparable ad, ranking it as a scam. The study did, however, provide useful information for categorizing fraudulent ads; nonetheless, it was limited to mobile phones, and more features are required for accurate fraud detection.

A rental fraud study was given in Van Der Zee et al. (2019), which requires the renter to pay in advance to rent a property on the UK's Craigslist website that does not belong to the scammer. The commercials are divided into three categories: authentic, phony, and uncertain. Pretending to be victims, I answered via e-mail with three messages to the thieves to urge them to send the money, and I discovered that the fraudsters' payment methods are Western Union and MoneyGram. They conducted 44 e-mail chats with the fraudsters and requested four real victims to fill out forms comprising personal information such as age, gender, career, education, and fraud questions. The data on which the study was based included e-mails and the first advertising, as well as questionnaire information from the four victims. They have categorized the fraudsters' persuasive strategies into ten social persuasion techniques. Yet, the study's major goal is to educate users on the persuasion strategies used by fraudsters in fraudulent leasing operations; however, the study did not address automatic ways for detecting deceptive adverts.

Marilyn A. Dyrud (2016) did a new study in which the author displays an analysis of Nigerian 419 letters, which is the fraud section of the Nigerian Penal Code, and they displayed the fraudulent ways Nigerians employ in their e-mails to induce the victim to send money to them. They employed the approach of sympathy to inflict on the victim, the other method is confidence, and the third strategy is an unmistakable call to greed. In summary, this study describes some of the strategies used by fraudsters to persuade victims and grab their money; however, no scientific studies are included in this study. It is merely a matter of studying the language of the identified bogus emails.

A study conducted by Garg and Niliadeh (2013) assesses the level of Craigslist fraud. vehicle and truck listings that are put under two categories: owner and dealer. The study was conducted in 30 cities across the United States, they collected data for recently published ads, they examined only by-owner classifieds, they used bad keywords, and their result was that only 1.7% of ads were flagged as scams, however, the study was only conducted in one type of ad and they used one category.

In this study, and after analyzing previous research and studying all of the methods used to detect fraud in internet ads, some signs indicating the presence of fraud in advertising were used, and these signs were insufficient to judge the presence of a suspicion of fraud. Some previous research uses traditional methods, which must be used as a preliminary analysis of advertisements before applying tools with sophisticated and smart components that automatically detect fraud by identifying the most important signs and following up on all the techniques used by fraudsters.

Discussions and research directions

Models based on fake signs

In this section, we build a taxonomy for detecting fraudulent ads based on the relevant studies mentioned in the preceding sections. We classify models and techniques based on the methods and signs used to detect fraud. We compare the effectiveness of fraud detection techniques and the impact of impostor signals at a high level. In addition, we categorize each architecture based on a set of standards for the technologies and methods used in fraudulent advertisements. Table 3 lists the most common scam warning signs. Moreover, we carefully examine and analyze the signs that indicate the presence of fraud, as well as the extent to which they are currently used, and the possibility of using many signs in future studies to develop an integrated automated fraud detection system.

Previous studies to detect fraud did not focus solely on fraudulent advertisements. Internet fraud can take many forms, including romantic fraud,

Table 3. The most common signs of ad fraud.

Scam signs	Classified ad platforms	ad fraud tactics examined	Type of communication channel investigated in studies	References
VOIP, IP address contact phone number	Craigslist	Domain spoofing, Geo masking, Click spamming, ad stacking	Online dating, Email, IP address	(Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020; Minastireanu et al., 2019; Miramirkhani et al., 2017; Park et al., 2014; Vidros et al., 2017)
Common scam keywords	Craigslist	Domain spoofing, technical support scam, ad stacking	Online dating and ads	(Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020; Garg & Niliadeh, 2013; Kim et al., 2019; Miramirkhani et al., 2017; Vidros et al., 2017)
Ad images	Craigslist, online dating	Domain spoofing, ad stacking	Online dating and ads	(Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020; Al-rousan, Abuhussein, Alsubaei, Kahveci, et al., 2018, 2020; Suarez-Tangil et al., 2020)
Payment methods and transactions	Craigslist	Ad stacking, Geo masking, technical support scam	Online ads	(Miramirkhani et al., 2017; Park et al., 2014, 2017)
The price of the product	Craigslist	Cookie stuffing	Mobile phone	(Alsaleh & Zhou, 2018)
The physical address of the advertiser	Craigslist	Ad stacking, Geo masking	Online dating and ads	(Park et al., 2014, 2017)
Same Ad, multiple posting, same location	Craigslist	Domain spoofing	Online dating and ads	(Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020; Kharraz et al., 2018)
Scam emails	Craigslist	Geo masking, Domain Spoofing,	Online dating and ads	(Park et al., 2014; Sharifi et al., 2011; Sofo et al., 2010)

click fraud, and so on. Because all of these fraudulent operations are carried out over the Internet, the signs of fraud vary, but they are mostly similar in all of them.

The authors used image analysis technology and the frequency of these images in other ads through the URL to reveal the identity and identify the fake files in studies Al-rousan, Abuhussein, Alsubaei, Kahveci, et al. (2020), Al-rousan, Abuhussein, Alsubaei, Collen, et al. (2020), Kharraz et al. (2018), and Suarez-Tangil et al. (2020), as images are an important marker through which fraud can be detected. The IP address and phone number are important indicators of fraud. In studies Online Card Fraud - FraudSMART (2021), Brown et al. (2007), Bashir and Robertson (2017), Amarasekara et al. (2020),

an analysis of the IP address and phone number was performed to determine whether this number belongs to the VOIP and is fraudulent or due to a real advertiser. In studies Garg and Niliadeh (2013), Al-rousan, Abuhussein, Alsubaei, Collen, et al. (2020), Kim et al. (2019), Miramirkhani et al. (2017), and Vidros et al. (2017), the authors analyzed the texts in the ads, whether in the e-mails or the ads themselves, to determine the common words that fraudsters use in their ads, which is an important guide for distinguishing a genuine advertisement from a fraudulent advertisement.

In studies Al-rousan et al. (2020) and Kharraz et al. (2018), the authors examined the images in advertisements by analyzing the texts within the images and determining whether these images belong to other advertisements or are not identical to the advertisement itself. The authors of study (Alsaleh & Zhou, 2018) focused on the price offered for the product as well as other advertisements similar to it because some advertisements have a very low price for the product on the market and are difficult to believe, raising suspicions of fraud. In studies Levchenko et al. (2011) and Li et al. (2012), the authors focused on DNS, domain, and Web crawler by crawling many well-known websites to collect ads and conducting field studies on them by communicating via email or phone with advertisers, specifically fraudulent advertisers, to try to determine which fraud methods they use as well as the domain name and server that fraudulent advertisers use. It is a forgery.

The most crucial factors that investigators can consider are the indications of fraud, the kinds of communication channels, and the fraud techniques employed by fraudsters. As a result, researchers try to concentrate heavily on these factors and gather as much data on them as they can. Earlier research prioritized domain spoofing over other fraud strategies like click spamming, pixel stuffing, and others Additionally, it concentrated on ways to communicate through online dating and paid less attention to email and phone use, despite the fact that the phone is the most popular way to communicate.

These studies show that some of them used a single sign or a set of signs that indicate the presence of fraud in the advertisement and that all of these signals are important and help in determining the reliability of the advertisements. It should also be noted that some of these signs are used in these studies in a traditional, rather than automatic manner.

Models based on detection methods

Traditional methods and field readings are used in many studies to analyze the content of advertisements and classify fraudulent ads. The tremendous development of the techniques used by fraudsters daily should prompt the development of new automatic methods that analyze all signs indicating the presence of fraud in advertising, classification, consumer education, and

Table 4. Methods for detecting deceptive advertisements.

Detection method	Conducted with an anti-fraud program or tools that exist in platforms or Browsers	Tools, algorithms, and features used	References
Traditional	No	Algorithms (Nave Bayes, J48, Decision tree, Random forest, Logistic regression) Tools (WEKA, Scam detection assessment)	(Kharraz et al., 2018; Kim et al., 2019; Levchenko et al., 2011; McCormick & Eberle, 2013; Sharifi et al., 2011; Vidros et al., 2017)
Automatic	No	Tools (Ekata, LWIS) Algorithms (Convolutional neural network, Deep neural network, Light GBM)	(Al-rousan, Abuhussein, Alsubaei, Collen, et al., 2020; Park et al., 2014; Suarez-Tangil et al., 2020)
The applied study, manual research	Two of six	Phone with fraudsters, interview with scammers, interview with victims, Email chats	(Alsaleh & Zhou, 2018; Button et al., 2014; Dyrud, 2016; Garg & Niliadeh, 2013; Miramirkhani et al., 2017; Park et al., 2017; Sofo et al., 2010; Van Der Zee et al., 2019)

consumer awareness of falling prey to fraud. Table 4 summarizes previous studies' methods for detecting fraudulent advertisements.

In the majority of the studies Minastireanu et al. (2019), Al-rousan, Abuhussein, Alsubaei, Collen, et al. (2020), Park et al. (2014), Huang et al. (2018), Miramirkhani et al. (2017), Li et al. (2012), and Suarez-Tangil et al. (2020), an automatic detection method for fraud is used. The process begins with the development of intelligent tools to analyze the content of advertisements in order to identify the most common signs of fraud and thus classify the advertisement as fraudulent. Few techniques (Kharraz et al., 2018; Kim et al., 2019; Levchenko et al., 2011; McCormick & Eberle, 2013; Sharifi et al., 2011; Vidros et al., 2017) used traditional methods such as crawling websites, collecting and studying ad fraud, as well as investigating people who have been exposed to a real fraud, to alert and educate consumers about the nature and type of fraud, as well as the methods used. As most of these studies are conducted on advertisements known to be fraudulent, the authors used the applied study, manual research, and field or online interviews with a group of advertisers in studies (Alsaleh & Zhou, 2018; Button et al., 2014; Dyrud, 2016; Garg & Niliadeh, 2013; Miramirkhani et al., 2017; Park et al., 2017; Van Der Zee et al., 2019). Information that assists in educating consumers and learning new signs that indicate the possibility of fraud.

Despite the presence of tools working on some sites to detect and prevent fraud such as (spam filtering, blacklisting of URLs, and site removal), fraud persists. This is because the technologies used by fraudsters are numerous and constantly changing, as well as a large number of advertising sites

and technological methods that are developing daily. This problem necessitates more studies focused on the methods used, as well as an attempt to define all signs of fraud using smart components such as deep learning and machine learning (Sharifi et al. 2011; Kharraz et al. 2018; Kim 2019; Vidros et al. 2017).

The artificial neural network has become extremely effective at classifying data, and one of the most important areas in which this algorithm should be used is to detect deceptive advertisements. Among the features associated with this data, specifically those that were frequently used in previous deceptive advertisements, such as domain spoofing (URL, IP address, …, etc.), and other such features, focusing on communication channels, specifically those used by fraudsters more than others, and developing a new modified algorithm for the neural network algorithm integration with tools used by popular ad sites to detect misleading advertisements.

Additionally, it is clear from earlier studies that few of them made use of anti-fraud tools or programs that can be found on websites like Craigslist and Amazon or in widely used international browsers like Google, which will support the methods used in these studies for identifying fraudulent ads and groups. As the authors could use a combination of algorithms to classify the data and detect fraud, as well as useful feature selection on the available data and train on this data in various ways and with a set of algorithms, the majority of the algorithms that were used in the traditional methods were also insufficient or performed indirect ways. In order to increase accuracy, it is possible to use deep machine learning techniques in conjunction with manual research to compile data on previous fraudulent advertisements, accounts that defrauded victims, individual accounts of fraudsters, and the use of automated tools by well-known websites.

Conclusions

Although eliminating ad fraud is challenging, there are strategies to avoid ad fraud. Furthermore, it is the responsibility of the ad technology sector to maintain a safe environment for all parties, including publishers, advertisers, and consumers. To keep ahead, publishers must collaborate with advertising companies that specialize in combating advertising fraud in addition to employing procedures that are the first line of defense against advertising fraud.

In this survey, we established a two-level classification approach for fraud detection methods in Internet ads. We used the most prevalent symptoms of fraud as well as the detection methods that are commonly employed in this industry. We also disclosed all of the notifications used by fraudsters in prior and actual frauds. Our findings have revealed some significant issues that require further research and examination. One of the major

obstacles is the rapid advancement of technology that fraudsters utilize on a daily basis, as well as their attempts to escape detection procedures. This allows future researchers to study alternative underused marks and to combine a bigger number of marks to safeguard and educate customers.

References

Almeida, P. S., & Gondim, J. J. C. (2019). Click fraud detection and prevention system for ad networks. *Journal of Information Security and Cryptography (Enigma)*, *5*(1), 27–40. https://doi.org/10.17648/jisc.v5i1.71

Al-rousan, S., Abuhussein, A., Alsubaei, F., Collen, L., & Shiva, S. (2020). *Ads-guard: Detecting scammers in online classified ads* [Paper presentation]. 2020 IEEE Symposium Series on Computational Intelligence (SSCI), Canberra, Australia.

Al-rousan, S., Abuhussein, A., Alsubaei, F., Kahveci, O., Farra, H., & Shiva, S. (2020). *Social-guard: Detecting scammers in online dating* [Paper presentation]. IEEE International Conference on Electro Information Technology, Chicago, IL (pp. 416–422). https://doi.org/10.1109/EIT48999.2020.9208268

Alsaleh, H., & Zhou, L. (2018). *A heuristic method for identifying scam Ads on craigslist* [Paper presentation]. Proceedings of the 2018 European Intelligence and Security Informatics Conference (EISIC 2018) (pp. 69–72). https://doi.org/10.1109/EISIC.2018.00019

Amarasekara, B. R., & Mathrani, A. (2016). *Controlling risks and fraud in affiliate marketing: A simulation and testing environment* [Paper presentation]. 2016 14th Annual Conference on Privacy, Security and Trust (pp. 353–360). https://doi.org/10.1109/PST.2016.7906986

Amarasekara, B. R., Mathrani, A., & Scogings, C. (2020). Stuffing, sniffing, squatting, and stalking: Sham activities in affiliate marketing. *Library Trends*, *68*(4), 659–678. https://doi.org/10.1353/lib.2020.0016

Andrews, L., & Boyle, M. V. (2008). Consumers' accounts of perceived risk online and the influence of communication sources. *Qualitative Market Research: An International Journal*, *11*(1), 59–75. https://doi.org/10.1108/13522750810845559

Arshad, A., Zafar, M., Fatima, I., & Khan, S. (2015). The impact of perceived risk on online buying behavior. *International Journal of New Technology and Research*, *1*(8), 263641.

Bashir, M. A., & Robertson, W. (2017). *A longitudinal analysis of the ads. txt standard*. https://cbw.sh/static/pdf/bashir-imc19.pdf

Beware of craigslist rental scams. (2021). https://sellbuymdhomes.com/real-estate-blog/craigslist-rental-scams/.

Brown, J. O., Broderick, A. J., & Lee, N. (2007). Online communities: Conceptualizing the online social network. *Journal of Interactive Marketing*, *21*(3), 2–20. https://doi.org/10.1002/dir

Buchanan, T., & Whitty, M. T. (2014). The online dating romance scam: Causes and consequences of victimhood. *Psychology, Crime & Law*, *20*(3), 261–283. https://doi.org/10.1080/1068316X.2013.772180

Button, M., Nicholls, C. M. N., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *Australian and New Zealand Journal of Criminology*, *47*(3), 391–408. https://doi.org/10.1177/0004865814521224

Castro, A. (2013). *The dangerous 419 spam*. https://archive.org/details/TheDangerous419.

Chaffey, D., & Smith, P. (2013). *Emarketing excellence*. https://charsoomarketing.com/wp-content/uploads/downloads/2016/02/Dave_Chaffey_PR_Smith_Emarketing_Excellence_Pl.pdf

Dash, A., & Pal, S. (2020). *Auto-detection of click-frauds using machine learning auto-detection of click-frauds using machine learning*. https://ijesc.org/upload/c85b77baa8fb8e66d83-d5a80fd11a744.Auto-Detection%20of%20Click-Frauds%20using%20Machine%20Learning.pdf.

Dave, V., Guha, S., & Zhang, Y. (2013). *ViceROI: Catching click-spam in search ad networks* [Paper presentation]. Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security (pp. 765–776). ACM. https://doi.org/10.1145/2508859.2516688

Dörnyei, K. R. (2021). Marketing professionals' views on online advertising fraud. *Journal of Current Issues and Research in Advertising*, *42*(2), 156–174. https://doi.org/10.1080/10641734.2020.1737276

Dyrud, M. A. (2016). *"I brought you a good news": An analysis of Nigerian 419 letters* [Paper presentation]. Proceedings of the 2005 Association for Business Communication Annual Convention, 2005.

Flasy, E. (2020). Survey on 'scams and fraud experienced by consumers'. Global Journals. https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/ensuring_aid_effectiveness/documents/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf.

Forsythe, S. M., & Shi, B. (2003). Consumer patronage and risk perceptions in Internet shopping. *Journal of Business Research*, *56*(11), 867–875. https://doi.org/10.1016/S0148-2963(01)00273-9

Garg, V., & Niliadeh, S. (2013). *Craigslist scams and community composition: Investigating online fraud victimization* [Paper presentation]. Proceedings of the IEEE CS Security and Privacy Workshops (SPW 2013) (pp. 123–126). https://doi.org/10.1109/SPW.2013.21

Hu, N., Liu, L., & Sambamurthy, V. (2011). *Fraud detection in online consumer reviews*. Institutional Knowledge at Singapore Management University. https://doi.org/10.1016/j.dss.2010.08.012

Huang, T. H. D., Yu, C. M., & Kao, H. Y. (2018). *Data-driven and deep learning methodology for deceptive advertising and phone scams detection* [Paper presentation]. Proceedings of the 2017 Conference on Technologies and Applications of Artificial Intelligence (TAAI 2017) (pp. 166–171). https://doi.org/10.1109/TAAI.2017.30

Jane, S., Buckley, M., & Greene, D. (2012). Expert systems with applications SMS spam filtering: Methods and data. *Expert Systems with Applications*. *39*(10), 9899–9908. https://doi.org/10.1016/j.eswa.2012.02.053

Järveläinen, J. (2007). Online purchase intentions: an empirical testing of a multiple-theory model. *Journal of Organizational Computing and Electronic Commerce*, *17*(1), 53–74. https://doi.org/10.1080/10919390701291000

Kharraz, A., Robertson, W., & Kirda, E. (2018). *Surveylance: Automatically detecting online survey scams* [Paper presentation]. Proceedings of the IEEE Symposium on Security and Privacy (pp. 70–86). https://doi.org/10.1109/SP.2018.00044

Kim, M., et al. (2019). *Scam detection assistant: Automated protection from scammers* [Paper presentation]. 2019 First International Conference on Societal Automation (SA 20196) (pp. 1–8). https://doi.org/10.1109/SA47457.2019.8938036

Lee, H., Lee, J., Kim, D., Jana, S., Shin, I., & Son, S. (2021). *AdCube : WebVR ad fraud and practical confinement of third-party ads*. https://www.usenix.org/conference/usenixsecurity21/presentation/lee-hyunjoo.

Levchenko, K., Pitsillidis, A., Chachra, N., Enright, B., Felegyhazi, M., Grier, C., Halvorson, T., Kanich, C., Kreibich, C., Liu, H., McCoy, D., Weaver, N., Paxson, V., Voelker, G. M.,

& Savage, S. (2011). *Click trajectories: End-to-end analysis of the spam value chain* [Paper presentation]. Proceedings of the IEEE Symposium on Security and Privacy (pp. 431–446). https://doi.org/10.1109/SP.2011.24

Li, Z., Zhang, K., Xie, Y., Yu, F., & Wang, X. F. (2012). *Knowing your enemy: Understanding and detecting malicious Web advertising* [Paper presentation]. Proceedings of the 17th ACM Conference on Computer and Communications Security (pp. 674–686). https://doi.org/10.1145/2382196.2382267

McCormick, A., & Eberle, W. (2013). *Discovering fraud in online classified ads* [Paper presentation]. FLAIRS 2013 – Proceedings of the 26th International Florida Artificial Intelligence Research Society Conference (pp. 450–455).

Minastireanu, E. A., Alexandru, U., Cuza, I., Mesnita, G., Alexandru, U., & Cuza, I. (2019). Light GBM machine learning algorithm to online click fraud detection light GBM machine learning algorithm to online click fraud detection. *Journal of Information Assurance & Cybersecurity*, *3*, 1–12. https://doi.org/10.5171/2019.263928

Miramirkhani, N., Starov, O., & Nikiforakis, N. (2016). *Dial one for scam: Analyzing and detecting technical support scams*. https://arxiv.org/pdf/1607.06891v1.pdf

Miramirkhani, N., Starov, O., & Nikiforakis, N. (2017). *Dial one for scam: A large-scale analysis of technical support scams* [Paper presentation]. https://doi.org/10.14722/ndss.2017.23163

Online Card Fraud - FraudSMART. (2021). https://www.fraudsmart.ie/stories/online-card-card-fraud/.

Park, Y., Jones, J., McCoy, D., Shi, E., & Jakobsson, M. (2014). *Scambaiter: Understanding targeted Nigerian scams on craigslist* [Paper presentation]. Network and Distributed System Security Symposium (pp. 23–26) https://doi.org/10.14722/ndss.2014.23284

Park, Y., McCoy, D., & Shi, E. (2017). Understanding craigslist rental scams. Lecture notes in computer science (including subseries lecture notes in artificial intelligence and lecture notes in bioinformatics), 9603 LNCS, 3–21. https://doi.org/10.1007/978-3-662-54970-4_1

Perera, K. S., Neupane, B., & Faisal, M. A. (2013). A novel ensemble learning-based approach for click fraud detection in mobile advertising. In R. Prasath & T. Kathirvalavakumar (Eds.), *Mining intelligence and knowledge exploration. Lecture notes in computer science* (Vol. 8284, pp. 1–12). Springer. https://doi.org/10.1007/978-3-319-03844-5_38.

Pi, S. M., & Sangruang, J. (2011). The perceived risks of online shopping in Taiwan. *Social Behavior and Personality: An International Journal*, *39*(2), 275–286. https://doi.org/10.2224/sbp.2011.39.2.275

Rastogi, V., Shao, R., Chen, Y., Pan, X., Zou, S., & Riley, R. (2016). Are these ads safe: Detecting hidden attacks through the mobile app-web interfaces (pp. 21–24). https://users.cs.northwestern.edu/~ychen/Papers/ndss16.pdf

Shaari, H., & Ahmed, N. (2020, December). *An extensive study on online and mobile ad fraud* [Paper presentation]. The Third Conference for Engineering Sciences and Technology, Elmergib University, Alkhoms, Libya (pp. 1–3).

Sharifi, M., Fink, E., & Carbonell, J. G. (2011). *Detection of Internet scam using logistic regression* [Paper presentation]. 2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC) (pp. 2168–2172). https://doi.org/10.1109/ICSMC.2011.6083998

Singla, R. (2018). *Chokegati: A browser extension to mitigate resource hints vulnerabilities in HTML5 Cyber Security Roshan Rangwani Supervisor*. https://norma.ncirl.ie/3563/1/roshanrangwani.pdf.

Smith, R. G., & Holmes, M. N. (1999). *Nigerian advance fee fraud* [No. 121]. https://www.aic.gov.au/publications/tandi/tandi121.

Sofo, F., Berzins, M., Ammirato, S., & Volpentesta, A. P. (2010). Investigating the relationship between consumers' style of thinking and online victimization in scamming. *International Journal of Digital Content Technology and its Applications*, *4*(7), 38–49. https://doi.org/10.4156/jdcta.vol4.issue7.4

Springborn, K., & Media, B. I. (2013). *Impression fraud in on-line advertising via pay-per-view networks impression fraud in online advertising via pay-per-view*. https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_springborn.pdf

Suarez-Tangil, G., Edwards, M., Peersman, C., Stringhini, G., Rashid, A., & Whitty, M. (2020). Automatically dismantling online dating fraud. *IEEE Transactions on Information Forensics and Security*, *15*, 1128–1137. https://doi.org/10.1109/TIFS.2019.2930479

Suresh, S., Di, F., Katerina, T., & Mark, P. (2019). An analysis of android adware. *Journal of Computer Virology and Hacking Techniques*, *15*, 147–160. https://doi.org/10.1007/s11416-018-0328-8

The most common examples of a phishing email. (2021). https://blog.usecure.io/the-most-common-examples-of-a-phishing-email.

Van Der Zee, S., Clayton, R., & Anderson, R. (2019). The gift of the gab: Are rental scammers skilled at the art of persuasion? (pp. 1–32). https://arxiv.org/abs/1911.08253.

Vidros, S., Kolias, C., Kambourakis, G., & Akoglu, L. (2017). Automatic detection of online recruitment frauds: Characteristics, methods, and a public dataset. *Future Internet*, *9*(1), 6–19. https://doi.org/10.3390/fi9010006

Whitty, M. T. (2013). Anatomy of the online dating romance scam. *Security Journal*, *28*(4), 443–455.

Zhu, Y., Byford, M., Gans, J., Weiss, A., & Xu, L. (n.d.). Acknowledgements: We are grateful for extensive comments and discussions with Simon An-derson.