# Towards the Development of Indicators of Fake Websites for Digital Investigation

**Mera Alremeithi [1], Aysha Alkuwaiti [2], Haya Alobeidli[3] and Richard Ikuesan**
Computing and Applied Technology, College of Technological Innovation, Zayed University, Abu Dhabi, United Arab Emirates

meralremeithi@gmail.com
ayshaalkuwaiti5@gmail.com
haya.alobeidli01@gmail.com
richard.ikuesan@zu.ac.ae

**Abstract:** A fake website is considered a website that is intended to cause harm and manipulate users, especially novice users without some knowledge of indicators of fakeness. Understanding the indicators of fake websites is thus considered an important concept to avoid being a victim of malicious attacks in online engagements. In some cases, such knowledge is required to reduce the potential attack surface of cyber criminals. However, the increasing rate of website diversity and complexities makes it difficult for an individual to distinguish between a fake and a real website while compounding the investigation process of a website. Also, the growing rate of website imitation technology and website domain closure presents a veritable platform for the development of fake websites. As a step towards determining the genuineness of a website, this study developed a forensic framework based on an exploratory analysis of different genres of fake websites. To achieve this, forensic methodologies and processes were applied to methodically selected samples of known fake websites based on three fakeness categories: Hoaxes, Cybersquatting, and Sweepstakes. The result revealed the existence of salient markers which can be used as indicators of fakeness and can be applied across a wide genre of websites. Furthermore, the resultant observation was used to develop a digital forensic framework for website fakeness evaluation. The developed framework was benchmarked to the ISO 27043/2015 and the NIST SP800-86 standard for completeness and relevance to forensic investigation processes. By leveraging the proposed digital forensic framework, an investigation can develop a reliable pointer to evaluate the genuineness of any website, which can significantly reduce the investigation time. For a non-forensic individual, the developed framework can be leveraged to identify, at first glance, the degree of fakeness of a website. Such a mechanism can therefore provide a useful tool to reduce the potential susceptibility of users thereby creating user awareness.

**Keywords:** Fake website, Hoax, Cybersquatting, Sweepstakes, Fake website indicators.

## 1. Introduction

There is a growing trend toward attacks that take advantage of the information present online to target human weaknesses. In electronic markets, fraud is a common challenge, and it affects various Internet consumers (Chua & Wareham, 2004). Asa significant source of online fraud, fake websites now generate billions of dollars in false money at the cost of unwary Internet users (Yue Zhang et al., 2007). According to a recent survey, fraudulent websites make up about 20% of the total Web (Gyongyi & Garcia-Molina, 2005). A random sample of more than 105 million web pages found that 35% of ".us" domain pages and 70% of ".biz" domain pages were fake (Ntoulas et al., 2006). Fake websites not only cause immediate financial losses but also have long-term trust-related effects on users that may make them reluctant to do further online transactions (Malhotra et al., 2004). Several classes of fake websites have been identified in the literature. Ranging from a phishing-induced website that seeks to exploit unsuspecting entities to hoaxes for disinformation (Abbasi & Chen, 2009; Chan, 2022; Frischknecht, 2021; Tacchini et al., 2017; Zahedi et al., 2015). A synopsis of the commonly encountered fake website is further presented in Table 1. The approaches leveraged to craft these websites can range from simplistic techniques to a multimodal complex approach.

**Table 1: Summary of Techniques used in commonly encountered fake websites.**

| Techniques/types | Description |
|---|---|
| Hoaxes | Creation of fake information websites for disinformation and other malicious act to deceive (or sway decisions in some instances) unsuspecting entities. |
| Cybersquatting | Cybersquatting requires the registration of domains that resembles existing popular/common trademarks with malicious intent. Examples include typosquatting, Homograph-squatting, Combo-squatting, Top-Level Domain-squatting |
| Domain spoofing | Also referred to as domain masquerading, and similar to typosquatting, is a form of fake website that involves the use of a similar domain (or email) address to an existing domain or email address to deceive an unsuspecting entity |
| Content spoofing | This technique, also called content injection, involves the injection of arbitrary content into a website to lure unsuspecting entities. |

| | |
|---|---|
| Sweepstakes | This technique leverages the unsuspecting entity's desire to win a lottery or some prized item. In this technique, an attacker could present a pop-up ad on the website to attract the potential of some prize and rewards for a given action. This action would ideally be genuine, however, used for malicious intent. |
| Scareware scam | This technique also leverages pop-up ads, however, with a psychological component that attempt to scare the potential victim to take an action. Such Ads would suddenly appear on a website with a dire warning and consequential non-committal thus, prompting the potential victim to act. This technique also leverages. Using this technique, other forms of scams be carried such as fake anti-virus software pop-up windows can be conducted. |
| Phishing website scam | This technique involves the use of a false domain that is similar in name and identity to an official website, thereby luring an unsuspecting entity into an illegitimate site. This technique often redirects the unsuspecting entity to the legitimate site after harnessing the login credential of such an entity. This can also be termed as a Counterfeit of a goods site. Attackers could further leverage this technique to conduct online shopping scams, Charity fraud scams, as well as health website scams. |
| COVID-19 Vaccine Trial Scam websites | This technique leverages the need for Covid-19 related information ranging from medical supplies, vaccines, and other medical-related equipment. This often involves the creation of a fake website with relevant details (often curated from legitimate websites) albeit, with malicious intent to unsuspecting entities. This technique can be used to craft several phishing scams as well as domain spoofing. |
| Advertising scam: Astroturfing | This technique utilizes a manipulative behavioral approach to artificially create an impression or disinformation to unsuspecting entities. The combination of this technique and other forms of phishing techniques can be used to generate a more complex fake website with a different audience as the target. A classic example of such is the Stock market scam where fraudulent entities present fake information and statistics about a given commodity to engineer fear and drift in market capitalization. Other forms of Stock market scams could include the development of a temporary website with fake information and rumor targeted at creating chaos, biased trading, and panic buying within a targeted market group. |
| Concocted website | This technique is used to develop fake sites that appear as legitimate commercial entities, which often pose as real escrow, financial, delivery, or retail companies. |
| Fake escrow websites | an escrow service is intended to serve as a trusted third-party protection against Internet fraud. A fake escrow website, therefore, acts in the same capacity, however, with a deviation from the standard of trust. |

Numerous solutions have been proposed for automatic fraudulent website detection in response to these worries (Li & Helenius, 2007). The majority are lookup tools that only use blacklists made up of unified resource locators (URLs) culled from member-reporting repositories kept by online trading forums. These systems are reactive by nature since they rely on user reports; by the time fake websites are added to the blacklist, many users have already encountered them (Neil Chou et al., 2004). A related family of systems employs proactive classification methods that can identify fraudulent websites without the aid of user reports. These systems make use of fraud signals, which are crucial design components of fake websites that could reveal their falsity. Unfortunately, contemporary classifier systems use extremely simplistic fraud triggers and classification assumptions, making them simple to evade (Li & Helenius, 2007). The detection of bogus websites is also a dynamic issue. Fraudsters frequently deploy new tactics and make use of more advanced technologies (Dinev, 2006). Systems for detecting fake websites have not been able to keep up with improvements made by its competitors. As a result, these technologies are not very good at identifying bogus websites, with most instances seeing detection rates below 70% (Yue Zhang et al., 2007). The types of fake websites that can be detected by existing methods are, thus, likewise constrained (Abbasi & Chen, 2013).

There is, therefore, still a demand for fake website detection tools that can recognize different types of fake websites effectively. This study explored the fakeness of websites from the forensic perspective with a core emphasis on recurring patterns in the different classes of fakeness. Given the numerous numbers of potential fake websites, this study further developed a selection criterion based on the aim of the study**.** Three types of fake websites were selected, which include: Fakeness due to hoaxes, cybersquatting, and sweepstakes.

## 2. Methodology

The overall process model followed to achieve this study is presented in Figure 1. It comprises three interconnected phases. The first phase presents the process of selecting a fake website genre. To enhance the forensic process of fake website detection, this study adopted the knowledge of inclusion and exclusion criteria

commonly used in design science research. To achieve this, carefully crafted inclusion and exclusion criteria for fake website exploration were developed, as presented in Table 2. By applying these criteria to the identified techniques presented in Table 1, this study further reduced the explored fake website techniques to be studied to three. To apply the selection criteria, all techniques identified in Table 1 met these inclusion criteria. Criterion IC6 was specifically considered for all the techniques. However, when the exclusion criteria were applied, the list was reduced to three. These include Hoaxes, cybersquatting, and sweepstakes. The selected techniques cover the general techniques for fake website development.

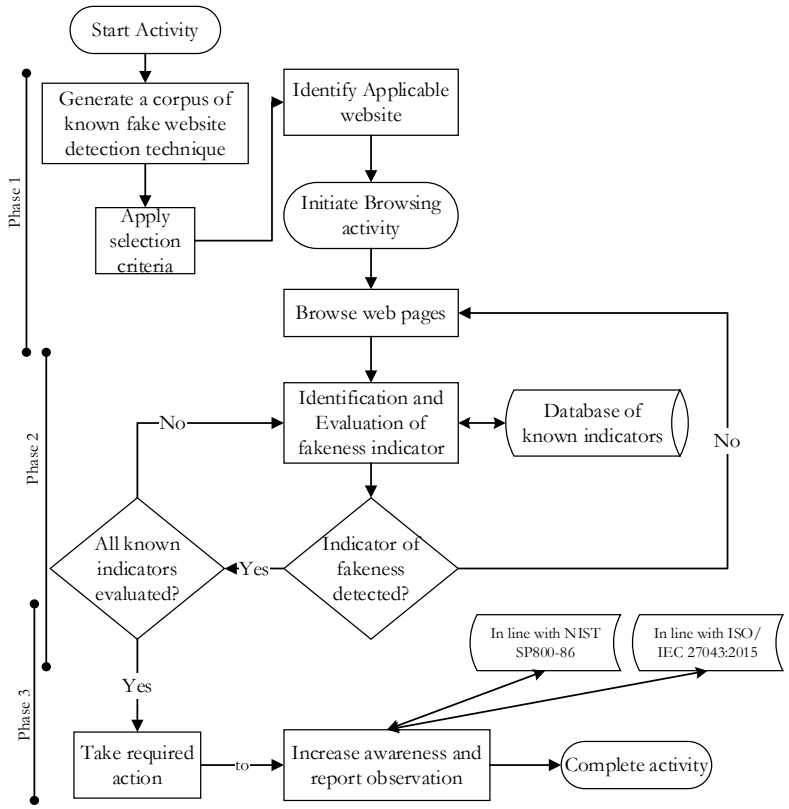


**Figure 1: Operational framework for an indicator of fakeness detection**

**Table 2: Selection Criteria for explored fake websites.**

| Inclusion criteria | Exclusion criteria |
|---|---|
| IC1: Potential to trigger a further attack or be combined to craft a more complex attack | EC1: Has been extensively studied in the literature |
| IC2: Performed with minimal effort and simplicity | EC2: Requires complex mathematical formation and modeling such as the use of machine learning and deep learning algorithms to detect |
| IC3: Pervasive and relatively common | EC3: Requires the use of a blacklist of either IP, URL, or other such properties for detection |
| IC4: Difficult to detect by an unsuspecting entity | EC4: Focuses on social media news only. |
| IC5: Prevailing technique despite an extensive awareness campaign | EC5: Potentially volatile such that relevant indicators may not available after the fact. |
| IC6: Focuses on websites. | |

In the second phase, an initial process a user may undertake is browsing the web. Primarily, the user might not recognize that the browsed website is a counterfeit. This phase of the process model provides a mechanism for evaluating the website for fakeness, by carefully comparing legitimate and fake websites for potential indicators of fakeness. By leveraging the forensic processes, an indicator of the fakeness database is further built, iteratively. The third phase considers the process of remediating fakeness exploitation. If a user discovers indicators on the website, they must ensure that all the indicators are studied and evaluated using the knowledge base. If all indicators are evaluated and any indicators match with the website, then the user is required to remediate through an awareness program. This approach can be used to prevent other users from

becoming victims of the website and report the detection of the indicators. However, if no indicators have been discovered, the user can continue browsing the web. Using this process model, as demonstrated in Figure 1, this study further conducts case studies with results presented in the subsequent sections. Primarily, the processes are evaluated in compliance with NIST SP and ISO/IEC standards.

## 3. Result and Analysis

Phases 2 and 3 of the process model presented in Figure 1 are applied to the three genres of fakeness in this section.

### 3.1 Understanding Indicators of Fakeness in Hoaxes

Without a doubt, it is well known that currently, we live in a fast-paced world where various events occur, and different news are spread online regarding these events. This caused misinformation to be formed and drastically spread among people digitally. When individuals are exposed to false information, it may lead them to perform actions that can cause them extreme damage. The terminology that describes this form of information is referred to as Hoaxes. A hoax can spread in different forms including fake information, virus messages, chain letters, or the spread of fake news websites. Hoax websites are created for reasons such as intentionally misleading the viewer, injecting malware, for political or financial gain, or spreading false information.

#### *3.1.1 Indicators of Hoaxes on Websites*

*a. Clear Signals:*

An obvious signal is that if the user is prompted to a site that requests to forward the statement to various people, it is clear it is meant to spread false information to many people. A hoax can be identified when it does not contain any credibility of the source information. Also, if a suspicious URL is included in the message, it is a direct identifier that it is a hoax since it could prompt the user to a fake website. Moreover, some statements are cleverly composed to grab the viewers' attention and provoke them emotionally to make the message seem believable.

*b. Impossible Statements and User Manipulation:*

A hoax aims to cause the recipient to be shocked by a warning that seems impossible to occur. Statements that seem impossible to believe are often spotted quickly. An example of an unreasonable message could be "A virus is detected, and it will cause fire and your computer will explode". Attackers usually create those alerts and make it seem that it is coming from an official organization.

*c. Fact-checking:*

In some cases, when a user is prompted to message or article that seems to be suspicious, an extensive fact-checking procedure needs to be implemented. It is recommended to check the source. For instance, the web address of the page should be inspected carefully because there might be spelling errors in the URL or domain name extensions. The authority of the page should be examined to determine if the mentioned author is real and credible.

#### *3.1.2 Case Study-1:*

During the spread of COVID-19 in 2020, cyber criminals exploited that period to create scams which led many people to be misled by those scams. Multiple organizations have created websites to display and track any statistics on COVID-19. However, cybercriminals came up with a method to take advantage of the coronavirus map websites. Attackers were able to design websites similar to the official pandemic maps that display statistics of the event. (Tangermann, 2020). The creation of such websites caused an increase in spreading false information regarding the virus and allowed hackers to obtain users' information. According to a security researcher, Shai Alfasi, attackers utilized these maps to discover the user's data (Mehta, 2020). The main malicious approach implemented by attackers was creating the coronavirus map websites that prompt the user to install an application to track any updates of the event. It was purposely designed this way by hackers to create a harmful binary file and download it to the user's system. The researcher has reported that hackers performed this technique by using software called AZORult. The software obtained information from the user's

computer including cryptocurrencies, passwords, installed programs, and stored account information (*Azorult Malware Information*, 2019).

### *3.1.3 Forensic Perspective*

From the concepts discussed so far, it is determined that the main indicator of hoaxes is by performing fact-checking. Therefore, a simple google search about tools or sites to use to identify misinformation would be helpful in this encounter. This seems a direct and clever approach to confirm the authenticity of a certain statement or story, however, not any fact checker site is trustworthy. It is undeniable that the number of misleading statements diffused in the online ecosystem not only confuses the viewer regarding the legitimacy of the information but also has doubts regarding the fact-checking sites that claim to be trustworthy. This brings us to an important aspect that we should be aware of which is that even the fact checkers' tools that seem to be legitimate are in need to be inspected. “Who inspects the fact-checkers?” is a question that is important to discuss when it comes to analyzing a source. Therefore, the presence of digital forensic approaches is required.

From a generic forensic perspective, there are basic approaches that are implemented. The study (Sousa-Silva, 2022) highlighted two generic techniques. The first approach mentioned is “human intervention” which involves human interaction with the data set to be examined. Human fact-checkers are recruited to confirm the integrity of the information. This approach may be useful in some cases; however, it has obvious limitations. Since facts are checked manually, generating results is a slow process since it is time-consuming. There is a high rate of producing inaccurate results because human fatigue is an expected occurrence. The use of this approach depends on the claim, the subject of the target, and how effective the fact-checking method is.

An alternative to the discussed approach includes the use of algorithms to indicate inaccurate content and verify sources (Sousa-Silva, 2022). The algorithm in this case focuses on the content of the data and the rate of content-checking accuracy instead of focusing on the sources’ reputation. Its emphasis is the message’s propagation dynamics in which the dynamics of the theory are being used to recognize the credibility of the information (Baror et al., 2020; Kebande et al., 2020). The main advantage of this technique is that it avoids any bias and can quickly process a humongous volume of data without the need for human interaction. All tools or mechanisms created so far to detect fake news properly, according to the author (Sousa-Silva, 2022), are not considered appropriate in the digital forensic field.

## 3.2 Understanding Indicators of Fakeness in Cybersquatting

Cybersquatting refers to a situation where a criminal uses, registers, or sells a domain name to benefit from another person’s or organization’s trademark (Mercer, 2000). The fast growth of the practice can be explained by the fact that most companies lack people who have deep technological knowledge. This observation has been evident since 2010 when cybersquatting started to affect the retail industry to a large extent, as demonstrated in the table below. In this case, the criminals' registered domains by using the names of certain popular companies to resell those later (Orduña-Malea, 2021).

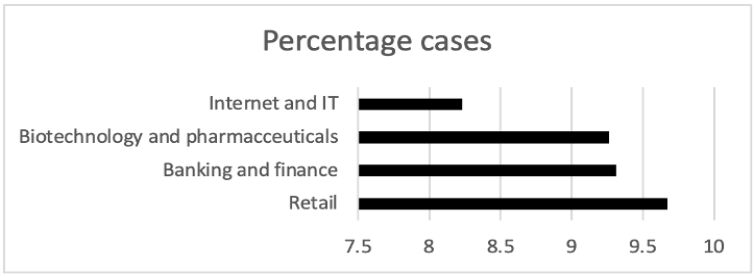


**Figure 2: Cybersquatting Effect on Different Industries (Petrosyan, 2022)**

### *3.1.4 Indicators of Cybersquatting on Websites*

Several indicators can reveal evidence of cybersquatting. The victims of the practice can identify it by searching for their domain names and looking for websites that mimic their platforms, have many ads but lack content, communicate negative information about their products, or have been under construction for a long duration.

*a. Identical URLs:*

The first indicator of cybersquatting is whether the desired URL leads to the domain page on sale instead of the unique website. Though this indicator may not independently prove a domain shark, it can point to a possible cybersquatting case, especially a type known as typosquatting (Agten et al., 2015). For example, a cyber-squatter who intends to hijack a site or a URL can simply aim to identify and convert Internet users' common typing mistakes. For instance, the squatters know that a person who intends to type www.buisness.com may type www.bizness.com or www.business.net, which comprise top-level domains. In this instance, the squatters will attempt to take advantage of a visual, logo, content, layout, color, sound, or hardware trademark similarities.

b. *Identical Products:*

The second indicator of cybersquatting is that the user will always be taken to a page that is promoting or selling related products. To achieve results, the criminal chooses a popular brand and associates it with similar products. This practice can benefit them since they use a long-term positive reputation of the products that another company provides. Consider as an example, company X sells medical devices, and website A sells related products and/or services, as well as having similar trademarks, content, and so on, then company X might be enduring a case of cybersquatting.

c. *Domain Name Displayed for Sale:*

Finally, other indicators become visible when the criminals attempt to proactively sell the site and try to overcharge their potential clients. In this case, the criminals are the ones who voice their intention to sell the domain before the owner expresses any interest to buy one (Chandra & Bhatnagar, 2019). The seriousness of squatting is demonstrated in the screenshot below, where cybersquatters are attempting to sell domains of a well-known landmark at an exorbitant price.

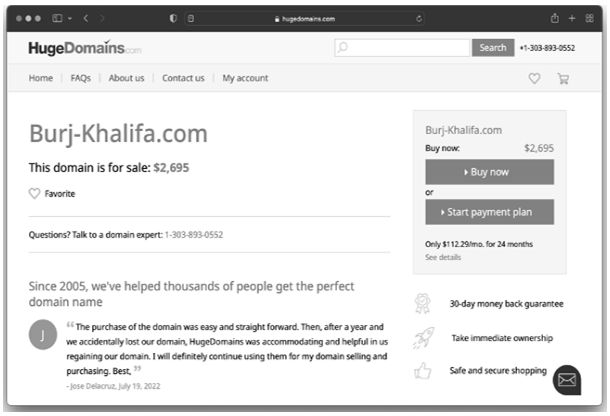


**Figure 3: Domain for Sale**

### *3.1.5 Case Studies-2:*

Among the common real-life case studies of cybersquatting is the case that pitted Tom Cruise against Jeff Burger in 2006. By the time Cruise learned about the crime, the squatter Burger had been using the domain based on his name (TomCruise.com) for over a decade (*Cybersquatting Examples: Everything You Need to Know*, 2022). A click on the website gives users an option of being redirected to watch the Top Gun Maverick 2022 new trailer. As a result of the *Tom Cruise v Operations Carter* case, the domain was transferred to Tom Cruise where he won the case.

In another case, a person has attempted to purchase domains to impersonate Amul which is one of the largest dairy firms in India, and created phishing sites. Amuldistributor.com, Amulboard.com, Amufran.com, Amufran.org.in, and Amuldistributorindia.com are examples of the sites to which Amul fell as a victim (Agarwala & Kang, 2021). To pull off their scam, the perpetrators created fictitious bank accounts in Amul's name, demanded money as a subscription to become an Amul distributor, and franchise-operated employment scams and demanded payment from applicants for job postings.

### *3.1.6 Forensic Perspective*

In most countries, the forensic tools to use, the specific indicators to focus on, and the application process to follow when investigating cybersquatting are indicated in a domain dispute resolution policy ("Domain Names and Cybersquatting," 2017). For forensic purposes, the authorities search for three major factors. The domain

name in question should be either confusingly similar to the service mark or a trademark of the complainant (Karanicolas, 2020). In addition, the registrant's interest in or right to the domain name should not be legitimate. Finally, the questioned domain name must have been registered and is currently being used for an illegal purpose or in bad faith (Radhika Vivek Bhusari & Karan Ramchandra Rampure, 2022).

Besides, there are multiple forensic tools available for performing a domain investigation, which seeks to determine whether a domain is authentic. Firstly, it is important to note that any domain usually has an IP address as well as host names that can legally send emails (Nangia, 2021). Secondly, it can be found in the Sender Policy Framework (SPF) record. As such, the process of investigating cybersquatting is focused on obtaining the IP address from which an email has been sent; then a verification process begins to confirm if it is like the emails in the SPF record (Singh, 2018). In addition, one of the online tools used in the investigation process is the Domain Name System (DNS), which helps in verifying the similarity between the suspicious and the authentic domain (Hewling, 2013). As a naming system, DNS allows users to reach any website by taking the keyed website name and redirecting the user to the IP address associated with it. The specific DNS tools commonly include DNSlytics, DomainEye, and Domain Dossier. For instance, the Domain Dossier tool creates reports from publicly available information on domain names and IP addresses to assist in problem-solving and cybercrime investigation. These reports could demonstrate the contact details for the domain owner, registry, and registrar details, as well as the organization responsible for hosting the website.

## 3.3 Understanding Indicators of Fakeness in Sweepstakes

Sweepstake scams are going widely distributed for a long time now, and yet, still they are going on strong. The initial contact in a sweepstake might be a notification you get while browsing a website that offers congratulations for winning a big contest. You will be asked to provide your bank account details. Once they have someone in their clutches, they will continue to contact them promising the big prize is just one more payment away. Most of the time common sense wins out and the customer recognizes that this is just another online scam. However, a less experienced user could not realize the threat until it is too late.


**Figure 4: A pop-up Sweepstake**

As shown in Figure 4, the user is tempted by the "Congratulations You Are Today's Winner" message. It's the ideal method for phishers to draw visitors into their web of deception.

### *3.1.7 Indicators of Sweepstakes on Websites*

A sweepstakes win would be a dream come true. However, if what you initially believe to be a genuine win notification turns out to be a sweepstakes fraud, your dream could become a nightmare.

*a. Sweepstakes demand payment to receive a prize:*

Scammers may claim that you must pay for the following before they will deliver your prize: Taxes on sweepstakes, Customs fees, Shipping fees, and service charges. If that's the case, you're probably dealing with a con. You will never be required to pay a charge to receive a reward in legitimate sweepstakes.

*b. The fact that you won a contest you didn't enter:*

You can only win sweepstakes that you have entered. It's a warning sign if you get a win notification from a contest that you don't recall entering. Take the time to conduct further research before you answer.

*c. Pressuring you to act in a hurry:*

Are you under any time constraints to reply to your win notification? If so, move cautiously. The reason why sweepstakes scammers want you to act quickly is so they can have your money before your check bounces.

*d. Asks you for your bank information:*

Does receiving your reward require you to validate your bank account information? This is blatant evidence of sweepstakes fraud. Legitimate sweepstakes don't require your credit card number for information verification. Your social security number is the only private data a trustworthy sweepstakes sponsor requires to handle your win.

*e. Sweepstakes scams don't know your first and last name:*

Does the title "Dear Winner" appear in your win notification? If so, this is a serious red flag. Numerous sweepstakes frauds send many letters or emails to every address they can find, without knowing any personal information. Genuine sweepstakes already have your entry information from the entry form.

*3.1.8 Case Studies-3:*

A crime was reported by GULF news in 2017 about a victim who clicked on a pop-up notification from a certain website as they claim he was the winner of 500,000 DH "in a lucky draw". He has been told to receive his prize; they should get his card details number including his pin. The victim proceeded further by giving them all the details about his bank account. After a while, he noticed that a withdrawal procedure was made from his card to an unknown person. At this moment, the victim realized that he was trapped in a fake prize situation. Directly he contacted Abu Dhabi police and by coordination with authorities, they managed to refund the victim's money back (*Police Warning on Fake Prize Win Scams*, 2017).

An incident happened in March 2022, Khaleej Times reported that Abu Dhabi has launched a big-ticket draw in which there was a real winner. They tried to contact her, but she refused to claim her prize because she thought those were scammers that would steal her money (Kumar, 2022). After this incident, Big-Ticket has established a rule where they will publish the winner's name on their website and their social media account to make it easier for people to believe them.

*3.1.9 Forensics Perspective:*

There are steps that the users could follow to be able to distinguish between the fakeness of websites, pop-ups, and sweepstakes. If the user has a popup notification on his screen while browsing a regular website, then, before proceeding with any step, the user must follow some instructions that are advised by a forensic investigator (A. R. Ikuesan et al., 2020; R. A. Ikuesan, 2016; Zawali et al., 2021, Latto, 2021).

a. Check the website safety:

Use a website safety checker like Google Safe Browsing to quickly determine whether a website is trustworthy. This is a wonderful website safety-check tool since, according to Google, their website checker "examines billions of URLs per day looking for harmful websites". Another option is by using the VirusTotal online tool. It scans websites using over 80 antivirus engines and URL blacklisting services.

b. Browsers safety tool:

The most used web browsers available today have security features. These built-in browser capabilities can disable Flash content, prevent dangerous downloads, block intrusive pop-up adverts, and much more. To implement the above features, the steps of the respective browser include:

i. In Chrome: Settings > Advanced > Privacy & Security
ii. In Edge: Settings > Advanced settings
iii. In Firefox: Options > Privacy & Security
iv. In Safari: Preferences > Privacy

c. Check the URLs:

A common technique used to evaluate website safety is to check a URL before clicking on it. Before clicking on a link, find out where it leads, to determine whether it is secure.


**Figure 5: Hovering a Mouse over a hyperlink.**

In Figure 5, an investigator can determine fakeness by hovering the mouse over any link, the URL must show in the bottom left of the browser. On the web, most users simply scan text. Because of this, hackers frequently use visually similar characters to mislead you into visiting their phishing websites and unknowingly providing them confidential information (for example, "Yah00.com" instead of "Yahoo.com").

d. Checking the website HTTPS:

Another technique to ensure a website is secure is to verify that it uses HTTPS whenever you visit it. The primary protocol for transmitting data between your web browser and the websites you visit is HTTP (Hypertext Transfer Protocol). The "S" stands for "secure," and HTTPS is simply a secure version. Check for the padlock in the menu bar of your browser to discover if a site is HTTPS-encrypted. If you see it, the website you're on is encrypting your connection to it with a trusted SSL cryptographic certificate. Furthermore, combining HTTPS encryption with a virtual private network (VPN) will increase your security because the VPN encrypts all of your internet traffic from the time it leaves your device until it reaches the website you're viewing and back.

e. Don’t trust the “trust” badges:

Trust seals or logos typically appear on retail or e-commerce websites to indicate reliability. These icons stand out as evidence of legitimacy to customers who scan the website. Although many trustworthy websites utilize trust badges as well, they are unofficially recognized. These icons are frequently copied and pasted on websites without any meaningful security. A trust badge offers no information regarding the security procedures of the site in question.

## 4. Discussion

The mentioned hoaxes indicators in the study; clear signals, user manipulation, and fact-checking are three significant techniques to directly recognize a hoax. These three approaches are generic ways that any individual can implement when dealing with a stated fact. However, limitations would exist if it only depended on these approaches. Therefore, in the digital forensic field, two generic approaches were mentioned, human intervention and algorithm observation; the latter approach is an alternative. It analyzes data by using algorithms offer the ability to process and handle a big amount of data and avoid any kind of bias. For future work, this strategy can be improved by creating a digital tool that performs the same function but is only used by experts checking to prove the credibility of a statement.

Apart from this, the fakeness of websites due to cybersquatting is a hurdle for both technical savvies and general users. Throughout the investigation implemented in this subject, few facts were discovered. Other than the fact that the domain used for cybersquatting might be similar to the targeted individual or business domain, there’s a specific type that is incredibly malicious. Homograph attacks in cybersquatting not only make the domain similar to the legitimate domain but also makes it the same. The secret behind homograph attacks is that cybercriminals change conventional domain names, which typically consist of ASCII digits, letters, and special characters, into domain names that graphically resemble valid ones using Punycode, which is a subset of Unicode characters. Subsequently, these malicious fake websites would be extremely hard to detect and differentiate, perhaps even when using the known indicators mentioned in the investigation. To exemplify, a study has been attempted by a man named Xudong Zheng. Zheng has bought a domain named “xn--80ak6aa92e.com”, and if a user clicked on this link, they will be redirected to a fake website that looks exactly like Apple.com besides the fact that the domain in the URL would appear as Apple.com.

Moreover, depending on the expansion of sweepstakes, people now are facing a horrific time to distinguish between fake and legitimate sweepstakes. To figure out the types of sweepstakes, we have discussed earlier the indicators that a user must focus on to identify a sweepstake. If a fake sweepstake was determined by the indicators, several tools would help the user by checking the reliability of each source. The online tools will be a great opportunity to figure it out. However, some tools can't determine the fake sweepstakes. Therefore, still, people are facing fake sweepstakes daily since there is no proven tool to ban those sweepstakes from showing up. To add up, there is one practice a user can do that wasn't mentioned earlier, which is to block the pop-ups from showing in the browser. Indeed, it's not a long-term solution, however, could save some money for some users.

## 5. Conclusion

In conclusion, although fraudulent websites are a widespread threat to Internet users, many still have trouble recognizing them. Any unreliable internet site that is used to trick people into engaging in fraud or malicious attacks is a fake website. Perpetrators take advantage of the internet's anonymity to hide their genuine individual motives in numerous ways. While there are many valuable things an entity can do online, not everything is as it seems. Websites created for a variety of criminal objectives can be found among the millions of legal websites competing for users' attention. From misleading information to committing identity theft, these fake websites attempt it all. The observation presented in this study can be applied to diverse other genres of fake websites. However, further studies are required to develop a comprehensive indicator of fakeness. This is particularly important when novel genres are developed by malicious stakeholders. Furthermore, a formal benchmarking of the identification mechanism with industry standards is a major component of the future work of this study. Such a mechanism can be deployed as an API for websites as well as plugins agnostic to web browsers.

## References


Abbasi, A., & Chen, H. (2009). A comparison of fraud cues and classification methods for fake escrow website detection. Information Technology and Management, 10(2-3 SPEC. ISS.), 83–101. https://doi.org/10.1007/s10799-009-0059-0

Abbasi, A., & Chen, H. (2013). *Detecting Fake Escrow Websites using Rich Fraud Cues and Kernel Based Methods*.

Agarwala, M., & Kang, S. (2021). Cybersquatting India: Genesis & Legal Scenario. *IJLMH*, *4*(5), 740–757.

Agten, P., Joosen, W., Piessens, F., & Nikiforakis, N. (2015). Seven Months' Worth of Mistakes: A Longitudinal Study of Typosquatting Abuse. *Proceedings 2015 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2015.23058

*Azorult Malware Information*. (2019, December 20). Trendmicro. https://success.trendmicro.com/dcx/s/solution/000146108-azorult-malware-information?language=en_US

Baror, S. O., Ikuesan, R. A., & Venter, H. S. (2020). A defined digital forensic criteria for cybercrime reporting. Proceedings of the 15th International Conference on Cyber Warfare and Security, ICCWS 2020, ii, 617–626. https://doi.org/10.34190/ICCWS.20.056

Chan, J. (2022). Online astroturfing: A problem beyond disinformation. Philosophy and Social Criticism, 0(0), 1–22. https://doi.org/10.1177/01914537221108467Chandra, R., & Bhatnagar, V. (2019). Cyber-squatting: a cyber crime more than an unethical act. *International Journal of Social Computing and Cyber-Physical Systems*, *2*(2), 146. https://doi.org/10.1504/IJSCCPS.2019.100197

Chua, C. E. H., & Wareham, J. (2004). Fighting Internet auction fraud: an assessment and proposal. *Computer*, *37*(10), 31–37. https://doi.org/10.1109/MC.2004.165

*Cybersquatting Examples: Everything You Need to Know*. (2022, September 2). Upcounsel. https://www.upcounsel.com/cybersquatting-examples

Dinev, T. (2006). Why spoofing is serious internet fraud. *Communications of the ACM*, *49*(10), 76–82. https://doi.org/10.1145/1164394.1164398

Domain names and cybersquatting . (2017). *European IPR Helpdeask*.

Frischknecht, P. (2021). Detection of Cybersquatted Domains (Issue July). University of Bern, Switzerland.

Gyongyi, Z., & Garcia-Molina, H. (2005). Spam: it's not just for inboxes anymore. *Computer*, *38*(10), 28–34. https://doi.org/10.1109/MC.2005.352

Hewling, M. O. (2013). Digital forensics: an integrated approach for the investigation of cyber/computer related crimes. *University of Bedfordshire*.

Ikuesan, A. R., Salleh, M., Venter, H. S., Razak, S. A., & Furnell, S. M. (2020). A heuristics for http traffic identification in measuring user dissimilarity. Human-Intelligent Systems Integration, 2, 17–28.

Ikuesan, R. A. (2016). Online Psychographic Model for Insider Identification [Universiti Teknologi Malaysia]. http://portal.utm.my/client/en_AU/main/search/detailnonmodal?qu=Online+data+processing&d=ent%3A%2F%2FS

D_ILS%2F0%2FSD_ILS%3A851360~ILS~0&ps=300Karanicolas, M. (2020). The New Cybersquatters: The Evolution of Trademark Enforcement in the Domain Name Space. *SSRN*, *30*.

Kebande, V. R., Karie, N. M., & Ikuesan, R. A. (2020). Real-time monitoring as a supplementary security component of vigilantism in modern network environments. International Journal of Information Technology (Singapore). https://doi.org/10.1007/s41870-020-00585-8

Kumar, A. (2022, March 9). *UAE: Dh100,000 Big Ticket winner refuses to claim prize, thinks organiser's calls are fake* . Khaleej Times. https://www.khaleejtimes.com/uae/uae-dh100000-big-ticket-winner-refuses-to-claim-prize-thinks-organisers-calls-are-fake

Latto, N. (2021, September 24). *Website Check — How to Check Website Safety | AVG | AVG*. AVG. https://www.avg.com/en/signal/website-safety

Li, L., & Helenius, M. (2007). Usability evaluation of anti-phishing toolbars. *Journal in Computer Virology*, *3*(2), 163–184. https://doi.org/10.1007/s11416-007-0050-4

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. https://doi.org/10.1287/isre.1040.0032

Mehta, I. (2020, March 11). *Hackers are using coronavirus maps to infect your computer*. The Next Web. https://thenextweb.com/news/hackers-are-using-coronavirus-maps-to-infect-your-computer

Mercer, J. D. (2000). Cybersquatting: Blackmail on the Information Superhighway. Boston University Journal of Science and Technology Law, 6(11).

Nangia, R. (2021). Cybersquatting From a Legal Perspective. *Legal Desire International Journal* , *8*.

Neil Chou, Robert Ledesma, Yuka Teraguchi, Dan Boneh, & John C. Mitchell. (2004). Client-side defense against web-based identity theft. *Computer Science Department, Stanford University, Stanford*.

Ntoulas, A., Najork, M., Manasse, M., & Fetterly, D. (2006). Detecting spam web pages through content analysis. *Proceedings of the 15th International Conference on World Wide Web*, 83–92. https://doi.org/10.1145/1135777.1135794

Orduña-Malea, E. (2021). Dot-science top level domain: Academic websites or dumpsites? *Scientometrics*, *126*(4), 3565–3591. https://doi.org/10.1007/s11192-020-03832-8

Petrosyan, A. (2022, July 20). *Leading industries with the largest share of domain name case filings due to cybersquatting as of June 2020*. Statista.

*Police warning on fake prize win scams*. (2017, November 12). Gulf News. https://gulfnews.com/uae/crime/police-warning-on-fake-prize-win-scams-1.2123257

Radhika Vivek Bhusari, & Karan Ramchandra Rampure. (2022). Cybersquatting: A Threat To The Globalising World. *Indian Journal of Law and Legal Research*.

Singh, H. P. (2018). Cyber Squatting and the Role of Indian Courts: A Review. *Amity Journal of Computational Sciences* , *2*(2).

Sousa-Silva, R. (2022). Fighting the Fake: A Forensic Linguistic Analysis to Fake News Detection. *International Journal for the Semiotics of Law - Revue Internationale de Sémiotique Juridique*, *35*(6), 2409–2433. https://doi.org/10.1007/s11196-022-09901-w

Tacchini, E., Ballarin, G., Della Vedova, M. L., Moret, S., & de Alfaro, L. (2017). Some like it Hoax: Automated fake news detection in social networks. CEUR Workshop Proceedings, 1960, 1–12.

Tangermann, V. (2020). *Hackers Are Using Coronavirus Maps to Spread Malware*. Futurism. https://futurism.com/the-byte/hackers-coronavirus-maps-spread-malware

Yue Zhang, Serge Egelman, Lorrie Cranor, & Jason Hong. (2007). Phinding Phish: Evaluating Anti-Phishing Tools. *Carnegie Mellon University*.

Zahedi, F. M., Abbasi, A., & Chen, Y. (2015). Fake-website detection tools: Identifying elements that promote individuals' use and enhance their performance. Journal of the Association for Information Systems, 16(6), 448–484. https://doi.org/10.17705/1jais.00399

Zawali, B., Ikuesan, R. A., Kebande, V. R., Furnell, S., & A-Dhaqm, A. (2021). Realising a Push Button Modality for Video-Based Forensics. Infrastructures, 6(4), 54. https://doi.org/10.3390/infrastructures6040054