6-2023

Tool to Detect Spam Websites

Durga Venkata Kaja

Susantha Herath
St. Cloud State University

Tool to Detect Spam Websites

By

Durga Venkata Sowmya Kaja

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science in

Information Assurance

June 2023

Starred Paper Committee:
Susantha Herath, Chairperson
Akalanka B. Mailewa
Jieyu Wang

Abstract

Traveling is about relaxing and not worrying about being scammed and losing money. The Internet is a wide place that is changing every day. Having a guide to navigate unknown places goes a long way to staying safe. In this paper, I have used several identifiers and provided analysis on the effectiveness of these identifiers. Travel Website fraud is a severe problem which is widespread around the world. Studies of travel scams are mainly focused on finding different ways that attacker's targets on the innocent travelers. Now the technology is advanced and that is causing newer and newer techniques to scam people. By illustrating the techniques to find such frauds and to prevent people from getting scammed is something this paper is trying to achieve. In this paper we will look at the various problems and preventive measures that need to be taken while browsing the internet. In this paper I will be talking about the tools I have used for analyzing a website. I will also be providing the analysis of the different identifiers in finding out if a website is fake or genuine. The results and the conclusions from the analysis can then be used in designing a safe tool which can be used for keeping the internet users safer and wiser. The safe rules can be used to develop browser addons, computer applications etc.

Table of Contents

Page

List of Tables

List of Figures

Figure Page

List of Graphs

Graphs Page

Chapter I: Introduction

Introduction

Criminals are confident to attack people in all the means of scams in various ways like while traveling, reserving tickets, tax filing, health insurance scams, reserving hotel scams and many more. These days, our work is wrapped up very fast with the help of the INTERNET. Skipping lines in the reservation center and being on the wait list for the phone calls is the biggest time-consuming task for everyone. Life has become very easy with the help of the internet. This is making the criminals or hackers work very easy to hack us by pretending they are from the real agency or organization.

This paper will focus on the Scams that are focused on traveling websites in all aspects like Hotel scams, Insurance scams, Cruse and many more. Traveling is the most favorite thing and well time spending event in everyone's life during holidays and they plan with their friends and families accordingly.

Taking this as an advantage hackers came into existence and frauds have become very common and many common people started getting effected by them. Fraud can be one of the main things in the world of the internet. There are various kinds of frauds involved like, internet fraud, credit card fraud, telephone fraud, website ad scams("An Introduction to the Different Types of Fraud," n.d.). These scams and frauds affect everyone in almost every part of the world. Like the hackers will post an ad to their mailing address or emails you or sending ads to your browser by saying that "you won a trip to Disney". By seeing this every one of us will be excited and start digging through the things on to get our free trip by contacting the people using email or telephone number which is given in their advertisement.

So, this paper will further discuss how these schemes are affecting people and how to solve them. To solve it a tool will be created to protect people from getting affected by these victims and scams. There are also various methodologies which will be discussed further in this project. The aim of the study and their main causes and how people got affected by this with a clear example were given in this project.

Problem Statement

In day-to-day life, the internet has become crucial. We interact with different websites and do many transactions. During the holiday time people plan for a vacation and start searching for vacation places, then deals, availability of tickets, car rentals on internet. There will be many pop-ups pop up adds like “you book a ticket and get a 5-star hotel for very less price, or you might also get some emails about the vacation deals. People fall victims and lose money every year by clicking these pop-ups, where these will direct the user to the fraudulent website. There it will collect all the personal information and payment information to make a reservation.

Individuals might also get calls from the scammers, pretending to be from the hotel’s front desk by offering room upgrades and requests to add their card in their hotel website.

Nature and Significance of the Problem

In the year 2021, a person started searching for vacation deals for their family and clicked the link that he got from a false travel agency. Users entered all the information asked on the website. After a couple of days, he came to know that his card entered in the travel agency website was completely swiped out. There will be no one to aid or help you in that stage or situation.

In my personal experience, during the COVID-19 pandemic I have seen many people who got affected by these vacation scams deals. They blindly entered the details of their credit cards by seeing “FREE vacation by just paying tax”. After a week they realized that they had got scammed and lost their money.

In USA, Bolster Research states that, travel scams have increased 4 times in the first 6 months of 2021, compared to the previous years("Travel Scams up 4x," 2021a).

According to FTC in USA shows that, nearly $75M are lost to vacation scams since start of COVID-19 pandemic (Wilson, 2021).

India, according to the survey of McAfee over 56.1% of people fall in victims which leads to the loss of millions of dollars to this vacation scams since long time (Rebello, 2019).

Objective of the Study

The object is to design and implement a tool that detects the Scam websites and provides ways of protecting the users falling from victims.

Study Questions/Hypotheses

Is this the only tool that finds the scammed websites?

How do you prevent users from Scams?

What are the mitigating techniques?

What other researchers have done?

How do users should protect themselves from being scammed?

What are the preventive measures?

Definition of Terms

Victims – a person who is tricked or made foolish.

Fraud – an individual or the company takes advantage of the customers by taking their private information or even access to their workspace or credit card details.

Scams – trick which is used to cheat someone out of something.

Tourist scams – people who are whiling to travel by falling themselves as victims

FTC – Federal Trade Commission – “It is an independent agents of United states government that shares jurisdiction over federal civil antitrust enforcement with the Department of Justice Antitrust Division”.*(Ftc - Google Search*, n.d.)

Travel/ vacation – A journey to a distinct place, Websites – it is a set of logs and pages that gives you much more information on what we are looking for.

COVID-19 – It is a disease that caused in humans by coronavirus that have symptoms like flu and severity of this will leads to death.

Spam, Spoofing sites, Airbnb, Uber.

Summary

In this chapter I have covered the introduction about what is a scam, how people are falling into victims by losing money. I have also shown the statistics on how many millions and millions of people lost their money in scams. We have also discussed the nature of the problem that really happened. I have also discussed the study questions on what we are going to discuss and work on further topics.

Chapter II: Background and Review of Literature

Introduction

This chapter gives in-depth knowledge on how the vacation scam deals happen, what are the various scams involved in vacation scams and how to overcome these scams. There are a few concerns that will be focused on this chapter by giving some real-time examples and events. Then the background related problem will be discussed further.

Background Related to the Problem

Earlier, people reserve tickets by going to a reservation office doing themselves by booking tickets manually by cash payment or a reputed travel agency, which is a safe way. Today technology has become vast and making all of us more comfortable by getting things done online. In shopping malls, we see stalls that have posters that say, “win a jackpot by entering to this lucky dip, entering your details to further contact you” this is one way for the scammers to get our personal information. After few days, we will get calls by discussing some other offers that are offered by the company. Here is where the scam comes into the picture. As going deep into this research, we found that scams in many ways like.

1) Scams in Ride sharing apps.

Uber and Lyft are the popular ride sharing applications which make a very user-friendly interface by just clicking a button to start your travel. But this comes with various scams around application.

Reader’s digest says that, in 2019 there is a complaint raised from many customers that random drivers are coming to pick-up riders who are waiting for their Uber and allowing only the cash paying method by the end of the ride. If you encounter such messages, that means it is scam (Papa, 2023.). They also heard about charging a few for cancelling the ride.

The most fishing scam that is happening every day in some part of the world is “Uber Cancellation Scam” (Schlappig et al., 2019). There are some situations where some drivers accept the ride but new show up the pickup point hoping that rider will cancel ride by them self and get some cancelation fee. If this is happening to mean a Scam by the driver of the uber and recommended to report to the Uber.

Fake Uber application targets many Android users who use some fake application detection like, Android fake app, Android Trojan malware and many more in the market. What happens is, when we down these applications on our smart phone, this app will launch a login screen that looks same as the original uber or Lyft application. Once the user enters his credentials then the malware launches the real application pretending that nothing suspicious had happened ("5 Uber Scams Everyone Should Be Aware Of" 2020). Now, scammers have your credentials, and they can access your account and see the personal payment contact information.

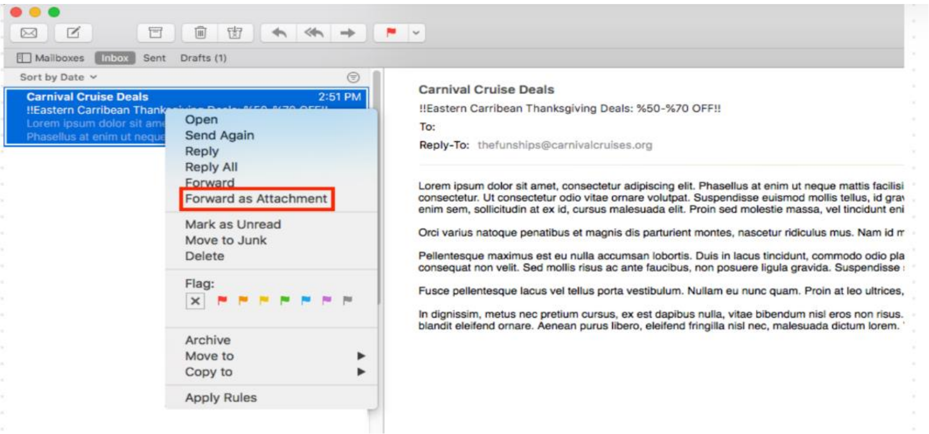
2) Cruise Scams:

Cruise scam is the dangerous scam which compromises your personal files, identity. An email is sent from the cruise line company, or some resort and a link also will be sent to your e-mail saying, “click her to win a free cruise for people of 2”. You might get the cruise emails from FedEx or UPS by saying something related to your upcoming shipment. ("6 Cruise Scams You Should Never Fall For", 2019)

The following fig depicts an example of a phishing email who is pretending to be a person from a Disney cruise.

Figure 1

("Report Email Abuse," n.d.)



Carnival Cruise Deals

!!Eastern Carribean Thanksgiving Deals: %50-%70 OFF!!

To:

Reply-To: thefunships@carnivalcruises.org

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Phasellus at enim ut neque mattis facilisi consectetur. Ut consectetur odio vitae ornare volutpat. Suspendisse euismod mollis tellus, id gra enim sem, sollicitudin at ex id, cursus malesuada elit. Proin sed molestie massa, vel tincidunt eni

Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Nam id m

Pellentesque maximus est eu nulla accumsan lobortis. Duis in lacus tincidunt, commodo odio pla consequat non velit. Sed mollis risus ac ante faucibus, non posuere ligula gravida. Suspendisse

Fusce pellentesque lacus vel tellus porta vestibulum. Nullam eu nunc quam. Proin at leo ultrices,

In dignissim, metus nec pretium cursus, ex est dapibus nulla, vitae bibendum nisl eros non risus. blandit eleifend ornare. Aenean purus libero, eleifend fringilla nisl nec, malesuada dictum lorem.

3) Travel Insurance Scam:

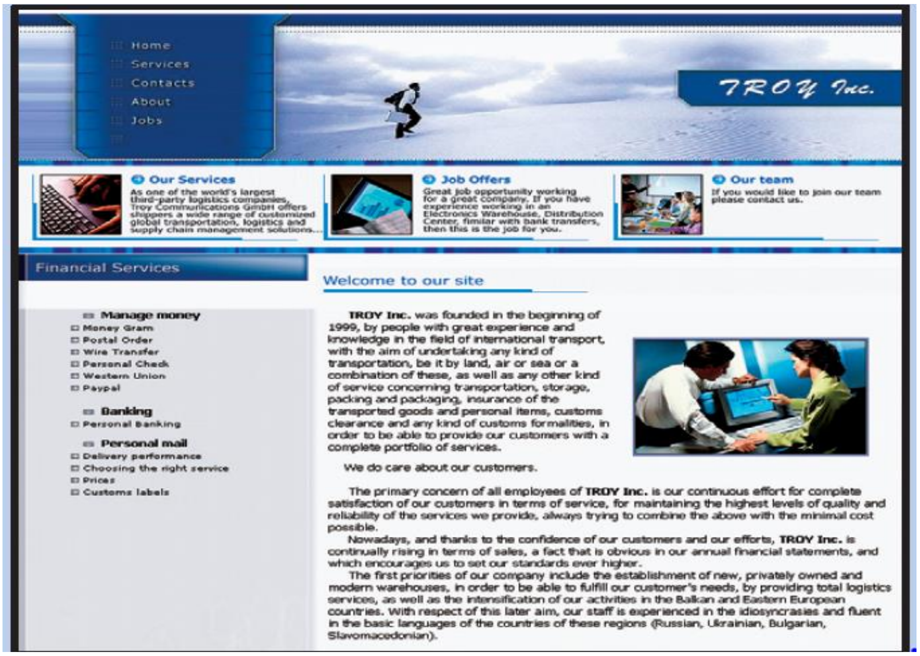
Travel insurance scams have become more common and widely spread all over the world. Because of this pandemic most of the world is kept in lockdown for about 4 months. That is the only time where the scammers are halt, but there have been no barrier to fraud.("Preventing and detecting travel insurance fraud Watson," n.d). “The pandemic has sadly provided more opportunities for scammers to target the travels” said by Hannah Isitt, travel expert at GoCompare, a UK-based insurance comparison site *(*"Which Nations Are on the UK Government’s Safe Travel List?," n.d.). Most of the fraudsters conduct the scam by pretending they are from a legitimate travel insurance company and talk with you in such a way that you can blindly trust.

There are various claims for insurance which are from lost luggage to medical insurance. As due to this pandemic and unexpected lockdown, traveling has become very unpredictable and most of the travelers are taking travel insurance. Most of the travel insurance is from a private company that got tied up with the travel websites. So, this type of fraud has increased more in the wider travel sector. Bogus websites and fake trave insurance companies are marketed more and have become more sophisticated for the past 18 months.

Marcus Liliana Rayos ("List of Scam Websites in 2019 (100% Proved) - TrackingMore," n.d.) is a person who got affected by this fake website and lots over $5K and here is the website that she got scammed from ‘bookmyairtravel.com’.

Figure 2

Travel Agency Spam Website



Our Services

As one of the world's largest third-party logistics companies, Troy Communications GmbH offers shippers a wide range of customized global transportation, logistics and supply chain management solutions...

Job Offers

Great job opportunity working for a great company. If you have experience working in an Electronics Warehouse, Distribution Center, fimilar with bank transfers, then this is the job for you.

Our team

If you would like to join our team please contact us.

Financial Services

Manage money
- Money Gram
- Postal Order
- Wire Transfer
- Personal Check
- Western Union
- Paypal

Banking
- Personal Banking

Personal mail
- Delivery performance
- Choosing the right service
- Prices
- Customs labels

Welcome to our site

TROY Inc. was founded in the beginning of 1999, by people with great experience and knowledge in the field of international transport, with the aim of undertaking any kind of transportation, be it by land, air or sea or a combination of these, as well as any other kind of service concerning transportation, storage, packing and packaging, insurance of the transported goods and personal items, customs clearance and any kind of customs formalities, in order to be able to provide our customers with a complete portfolio of services.

We do care about our customers.

The primary concern of all employees of **TROY Inc.** is our continuous effort for complete satisfaction of our customers in terms of service, for maintaining the highest levels of quality and reliability of the services we provide, always trying to combine the above with the minimal cost possible.

Nowadays, and thanks to the confidence of our customers and our efforts, **TROY Inc.** is continually rising in terms of sales, a fact that is obvious in our annual financial statements, and which encourages us to set our standards ever higher.

The first priorities of our company include the establishment of new, privately owned and modern warehouses, in order to be able to fulfill our customer's needs, by providing total logistics services, as well as the intensification of our activities in the Balkan and Eastern European countries. With respect of this later aim, our staff is experienced in the idiosyncrasies and fluent in the basic languages of the countries of these regions (Russian, Ukrainian, Bulgarian, Slavomacedonian).

4) Robotic calls Scam:

During the lockdown of this pandemic, precisely the incoming of the robotic calls has been dropped down. After the calming down of the pandemic, everyone started traveling and that returned of getting the robotic call travel scam. Most of the robotic scam calls say that you have won a free trip. These scams may involve low fair hotels, free food throughout your trip or even free cruise with just paying tax and maintenance fee. This is all because this scamming industry is trying to get your personal information and steal money over the phone. As per the research of Pauline Formmer, scammers are getting in touch with the victims pretending themselves as they are from a branded travel agency like, Priceline, Carnival Cruise Line, Hilton and many more ("With the Return of Travel Comes the Return of Robocall Travel Scams," n.d.)

5) Scams on Airbnb:

Airbnb has become more popular these days because of the convenience it provides. Most people prefer Airbnb rather than hotels as it provides a great way to live and enjoy the comforts of a home like kitchen. Travelers prefer Airbnb, and hence the scope for scammers has also been increasing.

I have listed most common Airbnb scams below,

i. Pictures look better than they appear: Using fake photos is more like a classic Airbnb scam. Scammers steal the pictures from the legitimate users and post those pics in their profile. You may find the picture resembles a star hotel and once you go to the vacation home it is totally different from the pictures posted. This is the most common scam which is implemented by many of the hosts to attract the tourists to their spot.

ii. Reviews are bad or good: Airbnb has many fake profiles, fake listings, and fake reviews. It is always advisable to check the reviews of the earlier guests before reserving your vacation home. Apart from that, you can also check if the identity of the host is a verified one or not. Usually, the host will need to give the government ID as proof of identity. If you didn't find the identity, then it's a scam.

iv. The host wants to communicate or pay outside of Airbnb: initially scammers might communicate via Airbnb, but after few days, they might communicate via emails, which is outside of the platform. Some innocent people will believe this is true and fall as victims and pay money completely outside the platform. After some days they might realize it’s a scam and they have fallen victim.

v. Listing seems perfect until you are there on the spot.

vi. Sudden cancellations due to plumbing issues:

As per the article ("Airbnb Scams L.A. Out Of $41 Million Each Year, Study Says," 2016). Some millions of dollars due to the issued of plumbing repair and if you contact the Airbnb people, they will give you a different hosting place with more expensive price and that turned to be a fake one.

vii. Double booking guests.

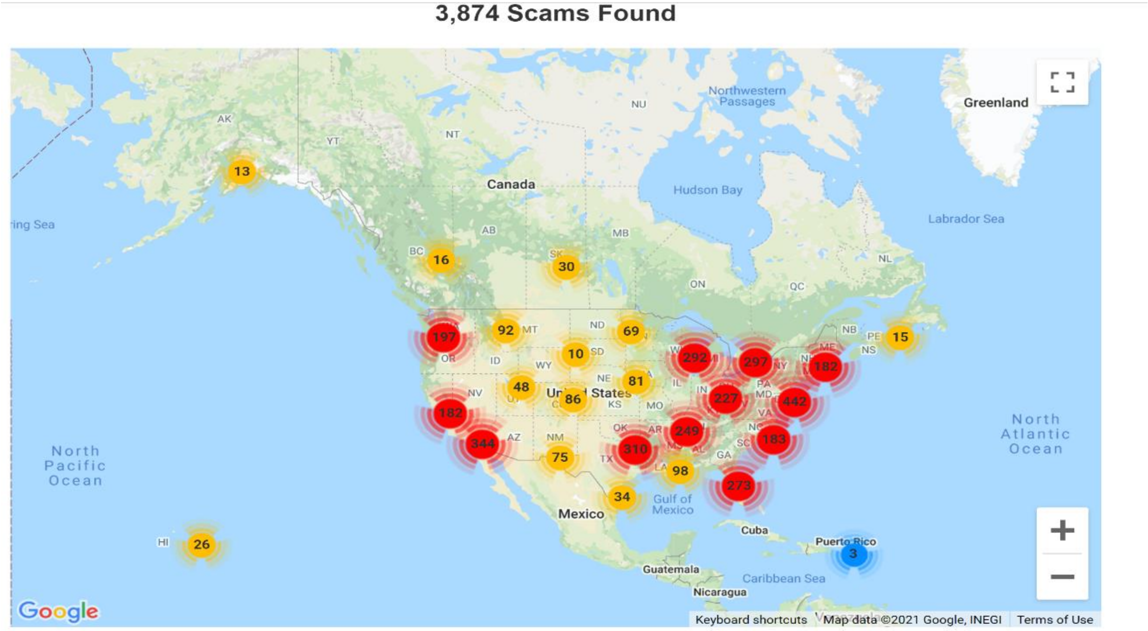
If you usually get a call from an unknown number and end up talking with you that, you won a free trip or a discounted trip by just attending a small meetup or attending the conference. Just hang up the call and report it to BBB.org. If you won or got a discount, you will get an official email from a registered organization.

Literature Related to the Problem

Behind every website scam, it involves more than $20Billion scamming industry. As of today, we suspect around 3,874 travel scams across the country (“BBB Scam Tracker^{SM}”, n.d.).

Figure 3

BBB Scam Tracker Detection On 12/14/2021("BBB Scam Tracker^{SM},"n.d.)



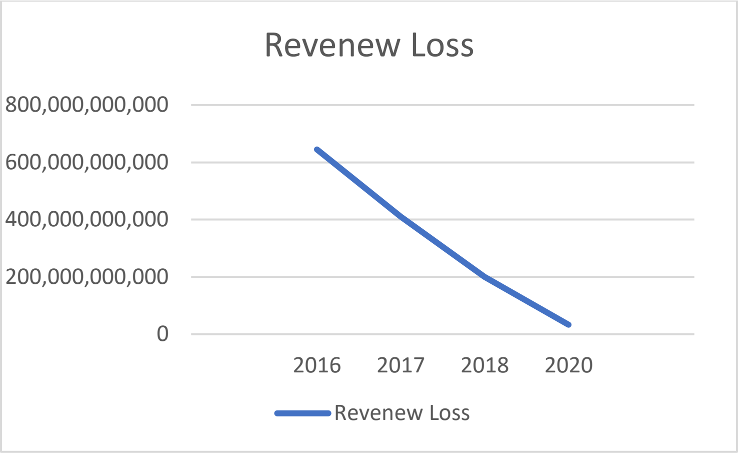
From the article ("25 Things About Airbnb Worth Knowing Before Booking," 2018), A person name Sarah Grossman found a perfect Airbnb for a wedding in Brooklyn. Since the listing said that you need to send me all the questions answered to a particular email, Sarah skipped the Airbnb platform and communicated directly via email. The fake host quickly responded that the apartment she is looking for is currently available. But they provided her with a bunch of other properties links. All the listings looked legitimate, and she didn’t even think it was a fake one. She then started booking the place by directly posting the money to the host via a different payment method. After a few days she came to know that that is scam, and she became a victim by losing more than 1000 dollars. She also listed the website that, she got scammed which is “AIRBNB.ITINERARY-BOOKING.COM”. The total scam revenue loss for victims is around $41 million dollars only in the place of Los Angeles, that deals with the plumbing issue ("Airbnb Scams L.A. Out Of $41 Million Each Year," 2016).

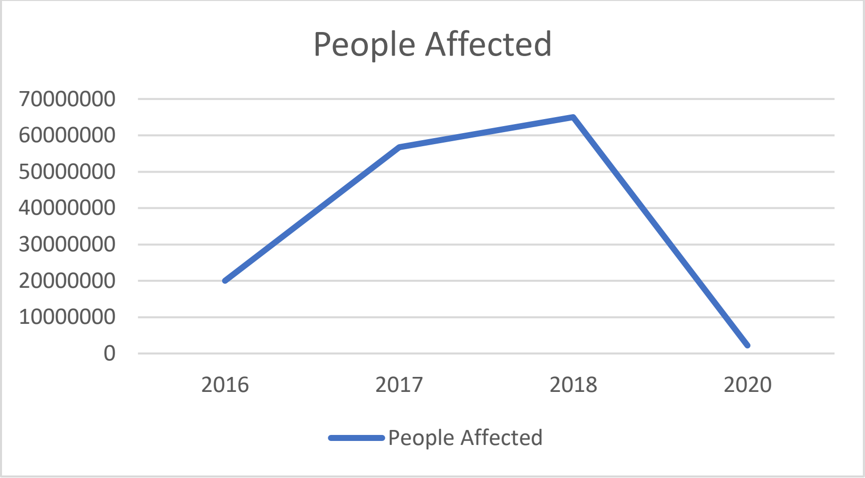
In 2015, at China a huge fishing emails and lots and lots of popups have reached to many people in China about the free Uber drive. Most of the people have raised complaints to Uber about the spam emails and pop-ups about the website they see. And uber have written a letter of these complaints stakeholders stating that, almost $1M scams have been listed per day for over a month ("This Driver in China Explains How He Is Helping Rip Off Uber," 2015). In the USA, Uber reported second quarter gross bookings of $21.9 billion, more than double the same period in 2020. Even so, the company posted the earnings loss of $509 million and a cash burn of $1.28 billion (Reuter, n.d.). As per the research of (Newcomer, 2017) Uber scams round the globe is about $645 Billion, where Billions of people got affected.

From the overall research of Uber scam, here is the graph on how the revenue loss for uber have taken place for the past 6 years:

Graph 1

Revenue loss and People affected





The article ("Planning a Cruise?," n.d.) the person named John, became victim to this cruse scam by clicking the pop-up. The pop-up says that “win a free cruse or a gift card for the Caribbean cruise in exchange of attending a meeting” by an attachment with a weblink “http://www.payssl-365.xyz/?fbclid=IwAR2lg_i1fCU0Hp1vEHBUW2Z48HcomMc2b9Zupm_c2towwm3X9Xschzb6snA” ("List of Scam Websites in 2019 (100% Proved)," n.d.).

As per the FTC over 2.2 million scams were reported, and the revenue loss is about $3.3 billion.

Travel insurance scam is a never-ending fraudulent scam, focusing on aged people and innocent people. As per the article of Europe in 2021(“Association of British Insurers,” 2021), a huge cheating scam have been pointed out on travel insurance which got increased 30% over the past few years. This scam files a revenue loss of over £1billion.

There are many scams involved in Airbnb mainly “plumbing problems”. In 2019, Airbnb have added more than 30% of new hosts ("3 Airbnb Scams You Need to Know About Before Booking Your Trip," 2021) which is like 7M worldwide of new listings have been updated.

Here are the few scammed websites I have found in my research:

- http://hiperfitd.com/?fbclid=IwAR3PmkV7n6xYnFBU-vKZtzPCdsSOZ5OkMUHLUpyeaZ_pXoSF_hx-kNJYEqc
- https://cclpay.com/?fbclid=IwAR2JWVxeQ-F0flMG_tAjXARM2U_lEcwEuKTLnKVpFNmOJjtq-L7Bxxdq1QE
- http://www.payssl-365.xyz/?fbclid=IwAR2lg_i1fCU0Hp1vEHBUW2Z48HcomMc2b9Zupm_c2towwm3X9Xschzb6snA
- This is a fake Airbnb website where Li have lost over 5,000 dollars “AIRBNB.ITINERARY-BOOKING.COM”.

Website looks like Airbnb but not:

- http://airbnb.com-request-trips.eu/online/listing/40c0bc/?rent=2126408?id=58038
- http://caribbeancl.com/index-3.html- cruise
- www.caribbeancl.com – cruise

Fake AIRLINE weblinks

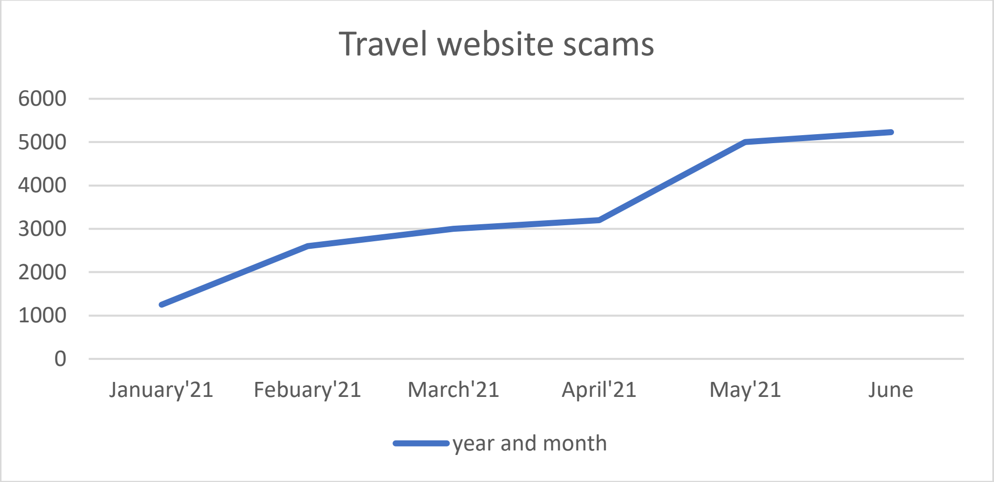
- https://checkphish.ai/insights/url/1619941479835/92c2f44e5737edb843f44189c278edd60fe6cb31350fafa97b82e7c256ca01a8 -- Suspicious American airlines webpage.
- http://abnb-rooms-192912.online/
- http://deltaair-lines-reservation.com/
- http://www.united-airlines-bookings.us/
- http://americanarflights.com/
- http://malware.wicar.org/
- www.flyfar.ca
- www.airfasttickets.com
- www.global-trips.com
- www.mytopdeals.net
- www.q3ea64.cn/YuzPo5Aj/tatamotorsinwyy/?_t=1681182358986#1681182361345
- www.flipkrt.com
- ww1.thegenis.com

- www.michaelkors-handbags.com
- www.pilosaleltd.com
- www.tiffanycoshop.com
- http://airbnb007.netlify.app.prostats.org/
- www.airbnb.place-online-search4491911.cc
- ww1.natwesti.com
- http://ww1.barclaya.net/
- http://ww1.lloydstsbs.com/
- ww1.barclays-supports.com

When pandemic took place in 2020, the scope for traveling have surged and for scammers, it became a very bad time due to lack of traveling. But in the year ’21, people started traveling a lot more than usual. Thus, travel scams have increased about 4 times more than then the usual. According to this article, ("TSA Checkpoint Travel Numbers," n.d.) number of travelers on the 1st day of summer is spiked which is 4 times which is 2.9M more than usual. From the recent article. During the 1st six months of ’21, the scam rate have increased ("Travel Scams up 4x as Pandemic Recedes and Travelers Take Flight," 2021b)

Graph 2

Scammed Sites In 2021



Literature Related to the Methodology

Scammers are getting innovative by creating fake websites, that seems to be realistic. They also use most reputative company names like pay pal, Alanita, Trip O ride and many more. To catch hold of scammers, software developer and the cyber security team got combined and invented many tools that detect malicious websites and protect everyone round the gold from not falling to victims. Here are a few fake website detection tools. From the research of (Abbasi & Chen, 2009) says that, fake website detection is of 2 system types: lookup and classifier (Zhang, 2022).

Table 1

Fake Website Detection Tool

Tool Name			Website Type	Previous Results Of Scam
	Classifier			
Calling id	Domain Registration Information		Scam Sites	Over All 85.9% Of Scam Detection
Earth Link	None		Scam Sites	Over All 90 % Of Scam Detection
Spam Fighter	None		Scam Sites	Over All 92.9% Of Scam Detection
Account Guard	None		Scam Sites Like Pay Pall, Amazon Pay, Zelle, eBay.	Over All 83.9% Of Scam Detection
Fire Phish	None		Scam Sites	Over All 89.9% Of Scam Detection
Cloudmark	None		Scam Sites	Over All 83.9% Of Scam Detection

Netcraft	Domain Registration Information		Concocted Sites, Scam Sites	Over All 91.2% Of Scam Detection
Anti-Phishing	Image Feature Similarity		Concocted Sites, Scam Sites	N/A
Site Hold	None		Scam Sites	N/A
Trust Watch	None		Concocted Sites, Scam Sites	Over All 85.9% Of Scam Detection
Spoof Guard	URL Similarities, DNS Valid registration		Scamming Sites	Over All 67.9% Of Scam Detection
BBB.org	Domain registration		Spoofing sites	Over All 99% Of Scam Detection
Scam-detector	Domain registration		Concocted Sites, Scam Sites	Over All 83.9% Of Scam Detection

For each tool in table 1 shows the type of the system, previous results, what type of website it is. The Lookup system uses a client server architecture to maintain the existing, blacklisted and known website URL's. Whereas Classifier system is an architecture based on the client side tools that applies the domain registration information.

Caller ID tool is a telecommunication tool that is developed in 1993, ("Caller ID," 2021) which is now updated as a True caller. It finds the fake callers, spoofing and displays Spam on your device.

Net Craft: Its evolution started from 1995 – 2021, still its updating and moving forward by helping people not to fall in their victims. This tool functions in such a way that it finds out the technologies that all the well-known websites use. It also depends on domain registration date, certification, website host and location.

Spoof Guard: it is a VM ware tool, which helps to prevent the website spamming and prevents us from phishing attacks (Ychin," n.d.). This tool is used to prevent sending traffic with IP address in your virtual machine. Spoof Guard also uses many webpage features like domain registration details and tries to figure out if it's a valid website or not.

Account guard: this is a server-side backlist tool that compares the URL of account registration form of the website with the trusted account registration of Amazon, PayPal or Wells Fargo sites and many more. This tool is powered by eBay,that showed a very good result of detecting fake websites.

Cloud Mark: it is developed in 2001, by Vipul Ved Prakash and Jordan Ritter. It is an anti-spam detecting tool that scans emails. The result is placed in the email header and mailed to the provider, it also have the fingerprints of that message ("What Is a Cloudmark Fingerprint and How Does It Work?," n.d.). This company protected more than a Billion people who got subscribers for the world's largest carrier network like AT & T, Airtel and Jio by protecting 12% of emails and more than 20% of messages ("What Is a Cloudmark Fingerprint and How Does It Work?," n.d.).

BBB.org/ scam tracker: It is tool with the huge organization that is recommend the victims to report they're in the following link,

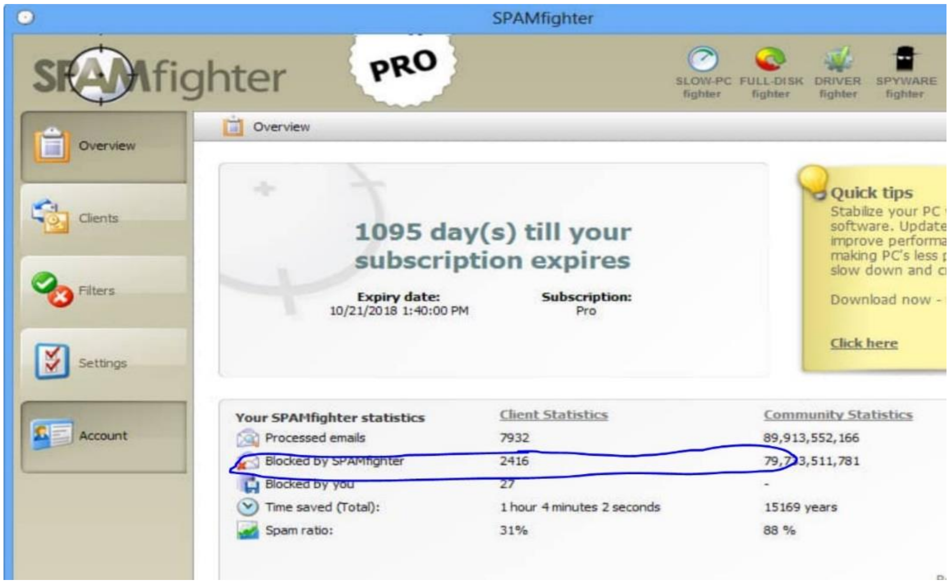
https://lifehacker.com/why-fake-travel-sites-are-fooling-more-people-1846792721.This way of providing the reports of the fake websites will help many people by not falling themselves as victims.

Anti-phishing: It is a client-side whitelist, which is a site watcher that observes all the image features, page style and the body text. It reduces the largest attack surface from the end users. It checks the link of the website and gives you a comprehensive report on the link we request.

SPAMfighter: It is a tool that prevents spam for Outlook, windows live, Thunderbird. This is a friendly tool that is user interface and easy to navigate. This supports multi languages. It is released in 2 different versions one is a paid one, which is SPAMfighter Pro and the other I am free version, SPAMfighter standard. If any of them is installed in your system, it will scan all the new and existing emails and search for scams in it. Once the suspicious email is found, it will add the sender to the backlist and block further emails from your inbox.

Figure 4

Spamfighter Demo ("*Spamfighter Tool - Google Search*," n.d.)



1095 day(s) till your subscription expires

Expiry date: 10/21/2018 1:40:00 PM

Subscription: Pro

Quick tips
Stabilize your PC
software. Update
improve performa
making PC's less
slow down and c
Download now -

Your SPAMfighter statistics	Client Statistics	Community Statistics
Processed emails	7932	89,913,552,166
Blocked by SPAMfighter	2416	79,7[illegible]3,511,781
Blocked by you	27	-
Time saved (Total):	1 hour 4 minutes 2 seconds	15169 years
Spam ratio:	31%	88 %

Spam-detector: Most of the fake spam websites seem to be looking like real ones which are TSA pre-check and Global entry. BBB says that criminals do this to rob money from innocent people. ("BBB Travel Scams Websites: Fake Travel," n.d). What this tool does is, if you enter the suspicious DN to the search bar, it goes into the website reviews of BBB and checks if the entered domain name of the link provided is a legitimate one or not.

Zero spam: this is a phishing email blocker. It is a cloud based antispam solution that protects us from Ransome wear attacks. All the emails with malicious links and text, this Zero spam will automatically block the sender and the attachments. Its main advantage is it runs on cloud, and it is powered by a network of 20 filtering nodes across 3 services. It also have a low-false rate("9 Best Anti-Spam Software & Tools For 2021", 2019).

Prevention Techniques

Firstly, there are some basic precautions that we can take to avoid fake booking sites. Check if the link provided in the email or the poster you received is a valid one. This can be checked as follows.

- See if the URL starts with https:// and should have a padlock icon on the address bar.
- Double check if you are clicking a valid link.
- Check the quality of site by finding how the text has been created, also a spell check of the website would help.
- It is important to check the suffix of the website as .com, .net, .org, .edu. If it comes to the government websites, it is mandatory to have a .gov suffix in their web address.
- It is always recommended to pay your bills using a credit card rather than the unknow 3rd party websites. Or can use the extended verification on payment gateways.
- If the communication is happening on emails or text messages, always ask for the ID proof and cross check in either Facebook or LinkedIn if they are the real people talking with you from the organization.
- Stop saving your back passwords and id numbers on your system.
- If you suspect a fraud just report it to “BBB.org/scam tracer”
- Download some licensed.
- Count the number of ‘/’s’ in URL.

Chapter III: Methodology

Introduction

In this part, I am going to discuss the objective of my project. Also, will explain my approach on how I am going to implement my tool. This chapter also covers the framework of my project, data collection, which environment am I going to implement the tool and what are the tools and techniques I am going to use to design my scam detection tool.

Design of the Study

In this, I am going to focus more on the approach on how to justify my research questions, which are mentioned in chapter 1.

1. Is this the only tool that determines the scammed websites?

   This can be found in various journals and articles. Apart from that, GOOGLE website is a huge source of lots of blogs that helped me in learning various tools that are available.

2. How do you prevent users from Scams?

   This one we can find in many official's blogs, and I found more of the prevention techniques in BBB.org. Studying various existing papers, journals and 100's of blogs also tells you some prevention techniques to the users.

3. What are the mitigating techniques?

   I have done this by collecting the data from the existing blogs, journals, and some I found in the google scholars from the time span of 2012 – present (2021).

4. What have other researchers done?

   The author of this article has done great work on finding the spoofing sights by using AZ protection system which uses the kernel-based machine learning classifier (Abbasi &Chen, 2009). What most of the other researchers have done is collect data from various articles and read reviews from various blogs and travel agencies. And a few articles of the researchers say that they have done the research by passing on the survey with a few questions related to the scams.

5. How do users should protect themselves from being scammed?

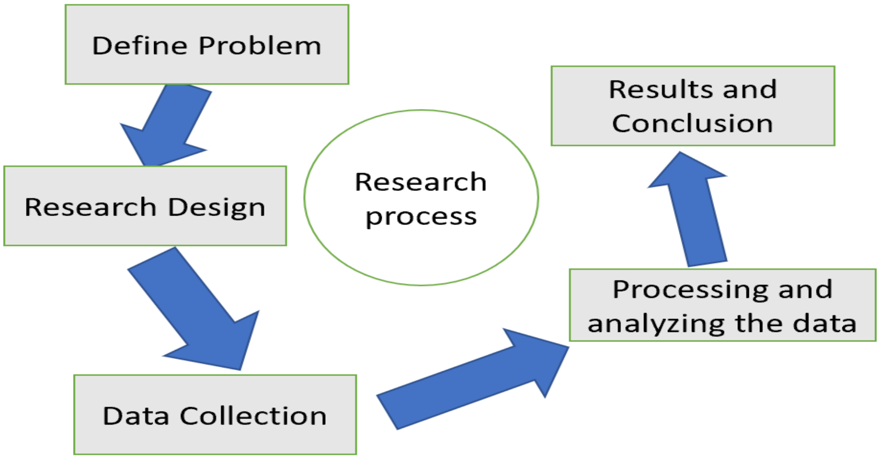
   The answers to this question can be found from various blogs and articles. BBB.org, FTC websites have handful of information on how to protect us from getting victims.

   In my study I am going to use the quantitative approach 80% and rest I have planned to use the qualitative approach. Therefore, my total focus of this project is to design a tool that helps common people. It is more objective, fast, and focused. And qualitative approach is used only when the scientist or the researcher don't have any idea of what they expect (Formplus Blog, n.d.)

My research process is defined as follows,

Figure 5

Research Process of My Project

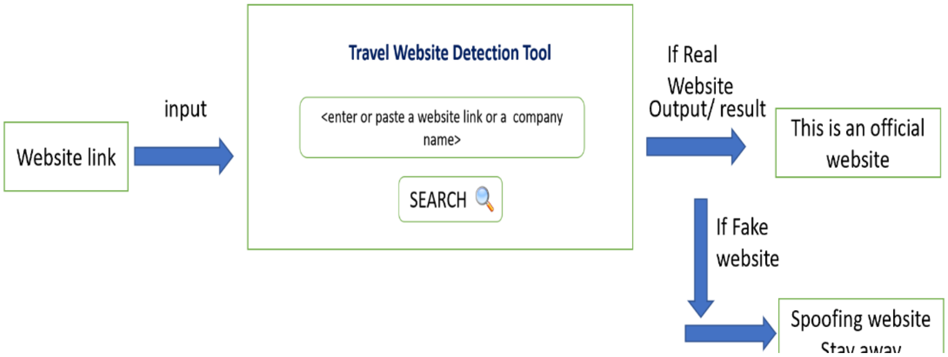


Data Collection

As mentioned in the study, data is found in various journals, new papers, articles, and the FTC website. I have collected many fake travel website links and the design of the tool will be described as shown in the diagram below. The detailed explanation of the data collection has been showed in Chapter IV.

Figure 6

Tool Design


Website link
input
Travel Website Detection Tool
<enter or paste a website link or a company name>
SEARCH
If Real Website
Output/ result
This is an official website
If Fake website
Spoofing website
Stay away

Tools and Techniques

Here in developing the tool I would like to pull the APIs from the existing well reputed tools. Then I will implement using java, java script, CSS, and spring boot.

Software Environment

I will be using IntelliJ IDE for implementing this project with Java-8, HTML, CSS, and Spring Boot framework.

Chapter IV: Data Presentation and Analysis

Introduction

Data analysis is a crucial part for presenting the findings of this Scam Detection tool. This analysis can further be used for developing more sophisticated tools. The tool UI is very intuitive and allows the user to make wise decisions to not get scammed. The purpose of this chapter is to present the data collected, the factors that affect the detection of scam websites. It presents the data that my tool collects, and shows the various methods used to analyze the data which detects potential scams. This chapter explores how I have gathered all the data and how my tool will identify the similarities and patterns to detect scam websites.

Data Presentation

How should we be able to identify the Fraud Websites? Do we have any tools available? The tool I have developed has all the information on how to avoid being SCAMED. A scam detection tool may be affected by several different attacks.

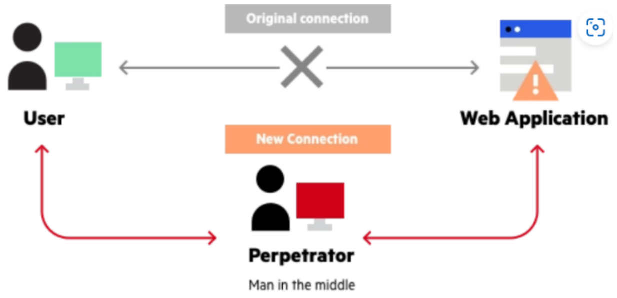
1. **Pay attention to the address bar - https or http**

   Always make sure to look up HTTPS in your address bar. It is not safer to click on websites that have HTTP. The website with HTTP doesn’t encrypt the data. which makes the website more vulnerable. When the website is encrypted, the data is been transmitted between the website server and the browser ("Scam Website Detector," 2022). While there are some legitimate websites that still use HTTP protocol. It’s always suggested neither not to click those websites nor enter personal information.

This involves MAN-In-The-Middle (MITM) attack. The goal of this attack is to rob the personal information of the user. The targets of this are on the commerce website, where login is required.

Figure 7

Man-in-middle Attack



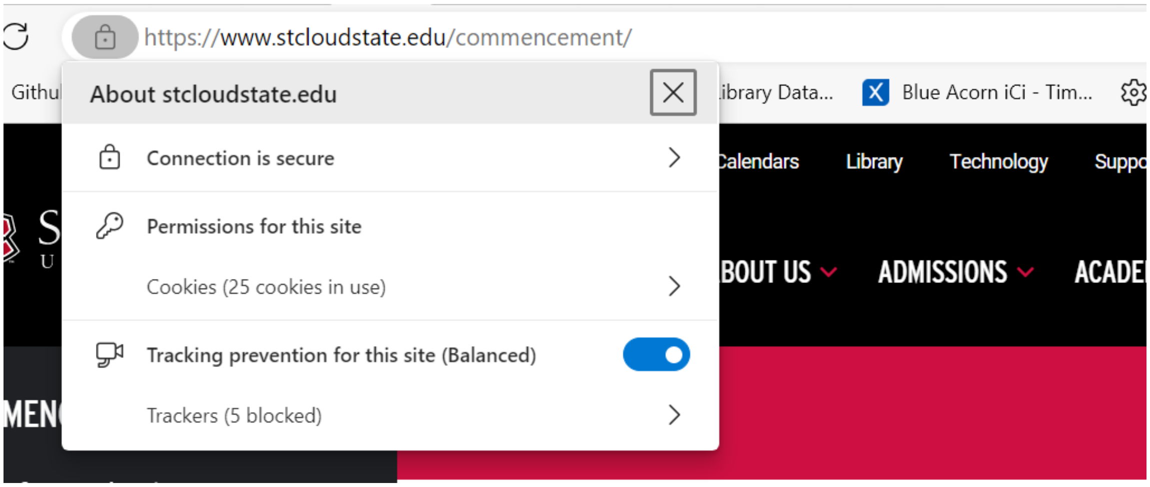
In HTTP website the data communication between the user browser and the server is passed on plain text, that helps user to read the login credits and could steal the data of user enters any banking information.’

2. **Be Aware of Padlock Icon.**

SSL is a Secured Socket Layer and TLS is a Transport Layer Security are two Security protocols which communicates over the internet. Make sure you have a lock icon on your address bar and check for the valid certifications on the browser as shown in the diagram.

Figure 8

Padlock and Certification Verification



https://www.stcloudstate.edu/commencement/

About stcloudstate.edu

Connection is secure

Permissions for this site

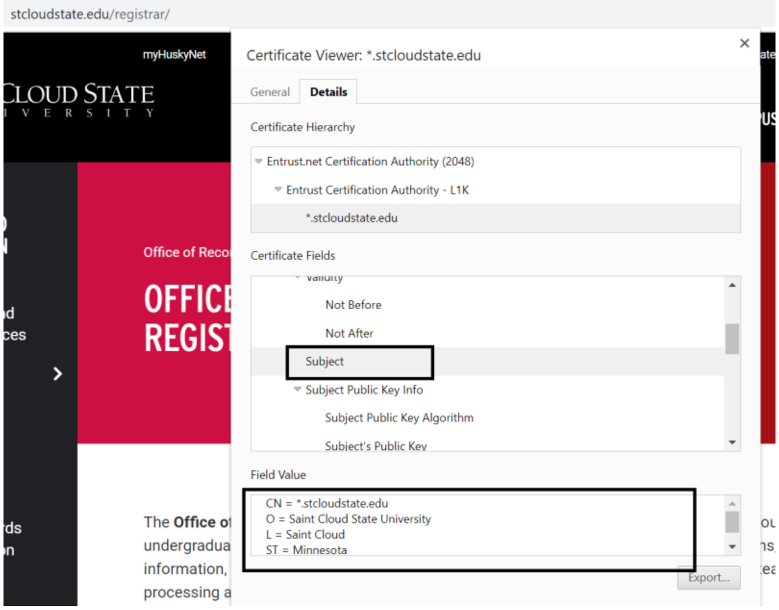
Cookies (25 cookies in use)

Tracking prevention for this site (Balanced)

Trackers (5 blocked)

Figure 9

Certifications Validations



stcloudstate.edu/registrar/

Certificate Viewer: *.stcloudstate.edu

General | Details

Certificate Hierarchy

- Entrust.net Certification Authority (2048)
  - Entrust Certification Authority - L1K
    - *.stcloudstate.edu

Certificate Fields

- Validity
  - Not Before
  - Not After
- Subject
- Subject Public Key Info
  - Subject Public Key Algorithm
  - Subject's Public Key

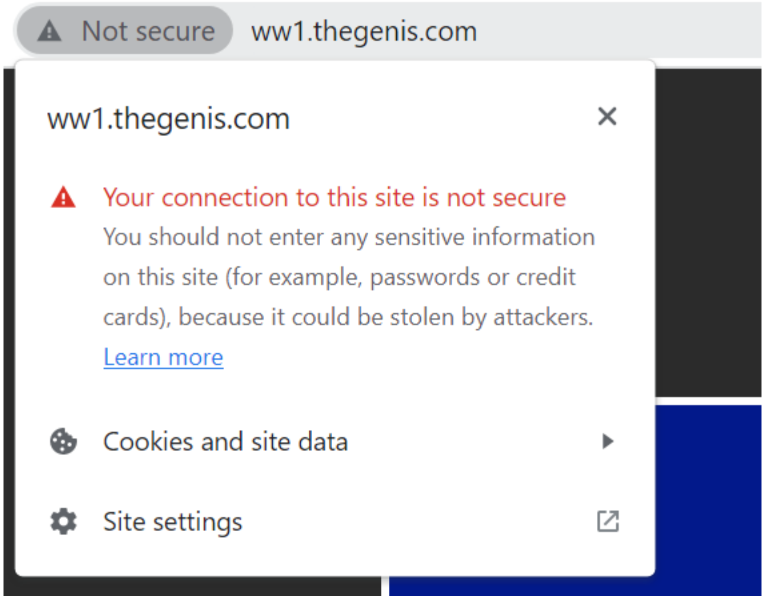
Field Value

CN = *.stcloudstate.edu
O = Saint Cloud State University
L = Saint Cloud
ST = Minnesota

The padlock indicates that HTTPS website is using an SSL/TLS encryption for protecting our data. SSL provides a high level of security which means it does have a valid certification for the website to determine if it's a valid website or not. Below is the screen shot for the insecure web page with no padlock.

Figure 10

HTTP Validations



Not secure ww1.thegenis.com

ww1.thegenis.com

Your connection to this site is not secure

You should not enter any sensitive information on this site (for example, passwords or credit cards), because it could be stolen by attackers.

3. **Spell Check using Google suggestions**:

Scammers make domain names that closely rep actual domain. They use some Unicode chars by doing that, domain name looked very closely with the real name. in my tool I provide top 10 suggestions for the user entered domain google regularly index the whole internet so these suggestions will represent the actual spelling of the desired domain by using this tool, a user can look at the provided suggestions and see is the domain is spelled correctly or not.

This will be very useful for finding out for misspelled domains. This is a widely used tactic to steal personal information, such as usernames, passwords, and credit card numbers.

To protect themselves from such scams, it is essential for users to be vigilant and verify the authenticity of any website or email they interact with. This can be done by carefully examining the domain name for any spelling errors or inconsistencies, and by being cautious of any suspicious messages or requests that seem too good to be true. By taking such precautions, users can minimize the risk of falling prey to scams that use misspelled domain names.

The API I have used is https://suggestqueries.google.com/complete/search?output=toolbar&hl=en&q=redif

The API I have used is https://suggestqueries.google.com/complete/search?output=toolbar&hl=en&q=redif

4. **Lookup domain details.**

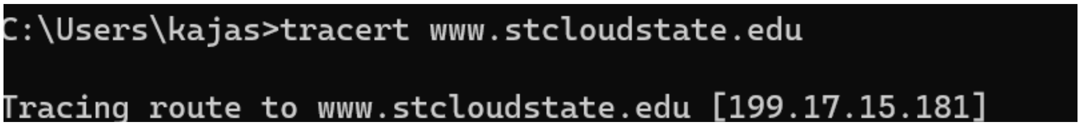
I used Tracert or traceroute Diagnostic tools to find out the IP address. *Tracert* - It allows to track the path of IP packet takes from the source server to the target device. It works by sending the TTL (Time to Live) values, which tracks the response from each device. The output of this device has a list of routers that pass the packets to the destination along with the IP Address ("What Is Traceroute? How It Works and How to Read Results," n.d.).

***Syntax**: tracert <URL>*

***Example**: tracert www.stcloudstate.edu**Example**: tracert www.stcloudstate.edu*

Figure 11

Implementing Tracert Tool



```
C:\Users\kajas>tracert www.stcloudstate.edu

Tracing route to www.stcloudstate.edu [199.17.15.181]
```

After capturing the IP Address, I wanted to get the domain details like server location, server address etc for the corresponding website. For this we found out various APIs for IP address look up as follows that supports V4 and V6:

i. *Domain Tools API:*

This is a popular tool which supports giving various information's on the domain. This API allows to get the website registration and expiration date and gives the DNS information. Here is the link to the API. https://www.domaintools.com/resources/api-documentationhttps://www.domaintools.com/resources/api-documentation ("API Documentation, " n.d.).

Pros:

- This tool has a wide range of filters and search options.
- Have very good and accurate and updated data about the domain name
- It allows us to track and monitor the changes that happen on the Domain name.

Cons:

- It's an expensive tool for an individual user.
- API Key is required for accessing.
- it needs a paid subscription for accessing various features.
- It has a trail version; a User could search only for 10 domain names per day.

ii. IP Info API

This API provides the geo location data for an IP Address like city, country, geo coordinates. This API accepts several parameters. An API token is required for all the requests. The API response would be a JSON/ XML/ CSV format.

API End Point is:

```
      https://api.domaintools.com/v1/DOMAIN/whois/history/
URI: /v1/{{QUERY}}/whois/history/  ("Whois History," n.d.)
```

It does a GET call to the IP Address server to pull the information.

The response to this API is as follows. ("Snapshot," n.d.)

```
{
  "response": {
   "record_count": 744,
   "history": [
     {
          "date": "2020-09-25",
          "is_private": 0,
          "whois": {
          ...
     {
          "date": "2020-09-24",
          "is_private": 0,
          "whois": {
            "registrant": "REDACTED FOR PRIVACY",
            "registration": {
     ...
          }
     }
   ]
  }
}
```

Pros:

- It’s an easy-to-use API.
- Offers a free plan.
- Give a fast response time and reliable data.

Cons

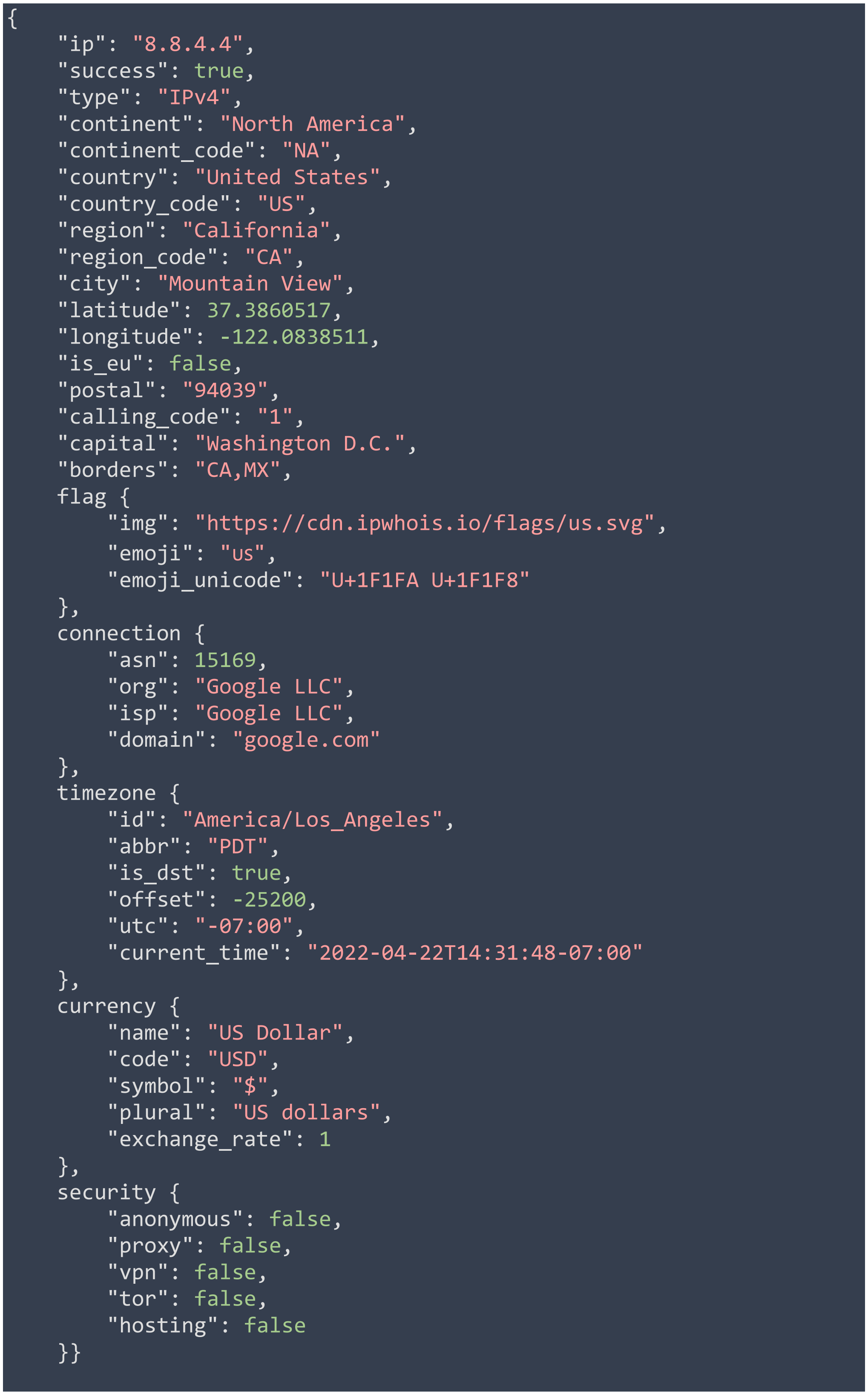
- Will not provide a detailed information for the domain search.
- We must have API credentials to use this API.

iii. *WHOIS API:*

A well-known API called WHOIS gives details about domain names, IP addresses, and other relevant data. With this API, you may look up information on a domain name, including who owns it, when it was registered and when it will expire, who to contact, and more (“IP Geolocation Documentation," n.d.). This API can be used to find domains linked to known malicious activity or with a pattern of abuse. You can spot changes in ownership or registration information that might show a domain has been taken over by a new owner for nefarious intents by looking at past WHOIS data.

Here is the documentation IP Lookup API and IP Geolocation Documentation (ipwhois.io). Here is the documentation IP Lookup API and IP Geolocation Documentation (ipwhois.io).

This API does a GET call to the IP Address server to pull the information. The response to WHO-IS API is as follows.



```
{
    "ip": "8.8.4.4",
    "success": true,
    "type": "IPv4",
    "continent": "North America",
    "continent_code": "NA",
    "country": "United States",
    "country_code": "US",
    "region": "California",
    "region_code": "CA",
    "city": "Mountain View",
    "latitude": 37.3860517,
    "longitude": -122.0838511,
    "is_eu": false,
    "postal": "94039",
    "calling_code": "1",
    "capital": "Washington D.C.",
    "borders": "CA,MX",
    flag {
        "img": "https://cdn.ipwhois.io/flags/us.svg",
        "emoji": "us",
        "emoji_unicode": "U+1F1FA U+1F1F8"
    },
    connection {
        "asn": 15169,
        "org": "Google LLC",
        "isp": "Google LLC",
        "domain": "google.com"
    },
    timezone {
        "id": "America/Los_Angeles",
        "abbr": "PDT",
        "is_dst": true,
        "offset": -25200,
        "utc": "-07:00",
        "current_time": "2022-04-22T14:31:48-07:00"
    },
    currency {
        "name": "US Dollar",
        "code": "USD",
        "symbol": "$",
        "plural": "US dollars",
        "exchange_rate": 1
    },
    security {
        "anonymous": false,
        "proxy": false,
        "vpn": false,
        "tor": false,
        "hosting": false
    }}
```

Overall, the WHOIS API can be useful for spotting potential scams, but it's vital to combine it with other techniques to gain a more complete view of a domain's reliability, such as website content analysis or reputation monitoring. Overall, the WHOIS API can be useful for spotting potential scams, but it's vital to combine it with other techniques to gain a more complete view of a domain's reliability, such as website content analysis or reputation monitoring.

This API gives the following information like, Website name, Domain Name, IP Address, Continent Name, Region, City, Country, Current Time, ISP Name and Domain Name. Which will be helpful for the user to see the information about the URL entered in the tool.

Pros:

- It’s a very easy integration with any application.
- Documentation has very good information about the integration with any application.
- Gives detailed information on the domain name.

Cons:

- This API Data may be unavailable due to privacy concerns or some data protection regulations.
- It is for the limited free usage.

6. Run A Virus Scan

Sometimes a false website's objective is to infect your device with malware rather than to steal your data, passwords, or money.

The pop-ups and ad-filled websites that hackers make can infect your phone or computer with viruses that enable cybercriminals to spy on you, search your device for sensitive information, or lock your device until you pay a ransom. Be sure your device hasn't been compromised if you recently visited a site like this ("How To Identify Fake Websites," n.d.)

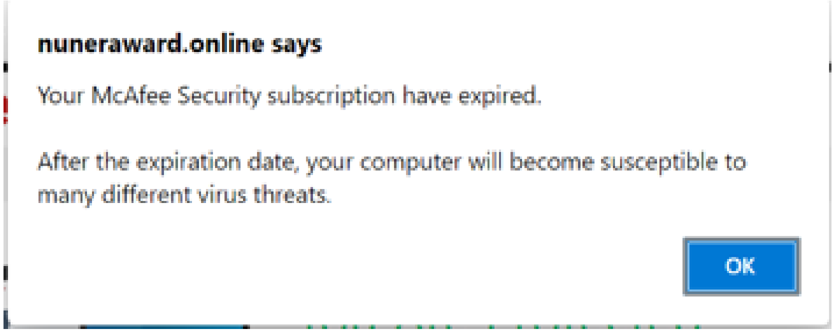
The antivirus software from Aura guards against hacking attempts and examines each of your devices for malware. Also, Aura can foreseeably alert you if you are about to visit a harmful or phishing website.

7. Pop-Ups And Ads:

Most websites online contain advertisements. However, if the website consists entirely of ads, you should not ignore them. These invasive ads can be difficult to remove since they either conceal their close buttons or lack them altogether. Additionally, the website may request that you enable browser notifications, and the page may only load after you comply ("Scam Websites," 2023).

Figure 11

Padlock Certs



nuneraward.online says

Your McAfee Security subscription have expired.

After the expiration date, your computer will become susceptible to many different virus threats.

Attacks Involved

The following common attacks may require protection from a fraud detection tool:

a. Phishing Attack:

Attacks involving phishing: Phishing is a form of social engineering in which the attacker tries to convince the victim to divulge personal information, including credit card numbers or login passwords. Phishing attacks are frequently sent via text message or email and may contain links to phony websites that imitate real ones. Sensitive data may be stolen because of a successful phishing attack and utilized for fraudulent purposes (“Threat Trends Report: Crypto Malware, Phishing, Trojans and More," n.d.)

Phishing efforts may need to be recognized and blocked by scam detection systems to prevent users from falling for these kinds of scams. This may entail looking for phishing indicators in emails or text messages, such as dubious links or requests for personal information.

This paper has my data collected information from the existing tools and consolidated into a few security points to show and let the user know what precautions need to be taken.

b. Malware attacks

Malicious software that infects a victim's device and steals personal data is used in malware attacks. Malware can appear in a variety of ways, including spyware, Trojans, and infections. Malware attacks, which can be launched via email, text message, or other channels, have the potential to infect a victim's device or steal important data (“What Is a Malware Attack? Definition & Best Practices," n.d.)

Users may need to be protected from these kinds of dangers by scam detection technologies that can recognize and stop malware attacks. This could entail looking for malware in files or URLs or applying heuristics to spot suspect activity.

c. ***Social Engineering Attack***

Scams on social media include phony giveaways and impersonation schemes, among other fraudulent actions that take place on these sites. As they frequently use social engineering techniques to dupe victims into revealing sensitive information or clicking on harmful links, these scams can be challenging to spot. (*PhishLabs - The Leader in Digital Risk Protection,* n.d.)

Social media scams may need to be recognized and blocked by scam detection systems to prevent people from being a target of these kinds of attacks. This can entail looking through social media posts for indications of fraud, such demands for confidential information or links to dubious websites.

d. *Vishing attacks*

Voice over IP (VoIP) technology is used in a specific type of social engineering attack known as a phishing assault to deceive a target into divulging critical information over the phone. Attacks known as "vishing" may use a fake caller ID or a plausible impersonation of a reputable company.

To shield users from these kinds of assaults, scam detection solutions might need to be able to recognize and stop vishing attempts. This can entail listening to phone calls for indications of fraud, like requests for private information or strange conduct. (*8 Examples of Vishing and How to Beat Them, n.d.)*.

e. Social media scams

Social media frauds involve fraudulent activities that occur on social media platforms, such as fake giveaways or impersonation scams. These types of scams can be difficult to detect, as they often rely on social engineering tactics to trick victims into providing sensitive information or clicking on malicious links.

Scam detection tools may need to be able to find and block social media scams to protect users from falling victim to these types of attacks. This may involve analyzing social media posts for signs of fraudulent activity, such as requests for personal information or links to suspicious websites.

Data Collected

I have gathered all the data and entered my tool, here is what I got the results as shown in the below table.

Table 2

Analysis of Websites

Website	Server Location	Padlock	HTTPS	Purpose	TLS/SSL certs	Misspelled	Virus scan	Asking for Personal Information	Pop-up and Ad's	Result
www.axisbank.co.in	India	Yes	Yes	Banking	valid	No	Good	Yes, Secured	No	Genuine
www.flyfar.ca	North America	Yes	Yes	Travel	not valid	No	Good	Yes, but Phishing	No	Fake
www.airfasttickets.com	Europe	No	No	Travel	valid	No	Good	Yes, Not Secured	Yes	Fake
www.global-trips.com	Europe	No	No	Travel	valid	No	Bad	Yes, Not Secured	Yes	Fake
www.mytopdeals.net	USA	Yes	No	Shopping	valid	Yes	Bad	Yes, Not Secured	No	Fake
www. smartfares.com	USA	Yes	No	Travel	valid	Yes	Bad	Yes, Not Secured	No	Genuine
www.q3ea64.cn/YuzPo5Aj/tatamotorsinwyy/?_t=1681182358986#1681182361345	N/A	Yes	No	Shopping	not valid	Yes	Bad	Yes, Not Secured	No	Fake

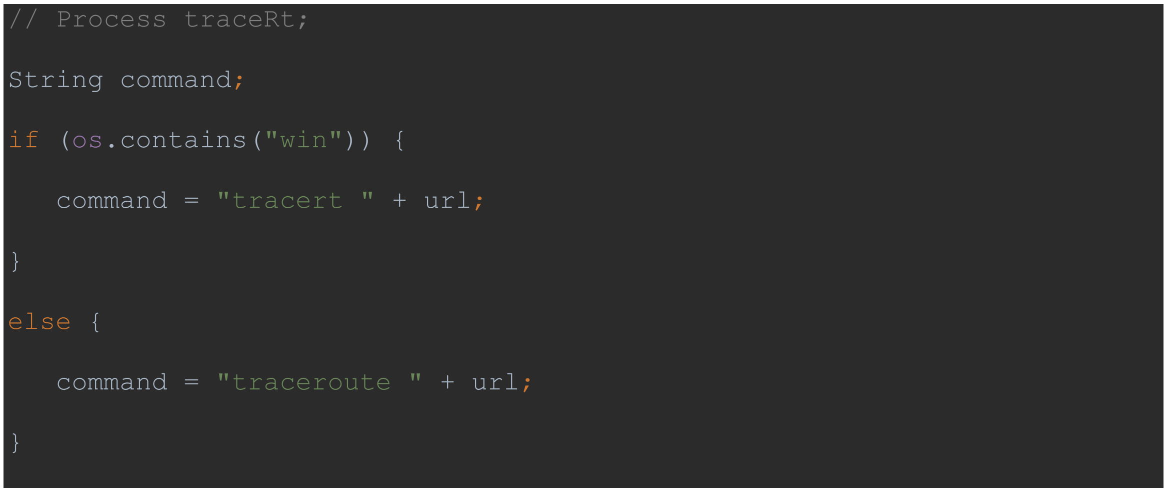
www.airbnb.com	USA	Yes	Yes	Travel	valid	No	Good	Yes Secured	No	Genuine
www.flipkrt.com	USA	Yes	Yes	Shopping	not valid	Yes	Bad	Yes Secured	No	Fake
https://www.flipkart.com/	India	Yes	Yes	Shopping	valid	No	Good	Yes, but secured	No	Genuine
ww1.thegenis.com	USA	No	No	Shopping	not valid	Yes	Bad	Redirecting to a different website	Yes	Fake
www.michaelkors.com	USA	Yes	Yes	Shopping	valid	No	Good	Yes, Not Secured	No	Genuine
www.michaelkors-handbags.com	Turkey	Yes	Yes	Shopping	not valid	No	Good	Yes, Not Secured	Yes	Fake
www.pilosaleltd.com	Canada	Yes	Yes	Shopping	not valid	Yes	Bad	Yes, Not Secured	No	Fake
www.tiffanycoshop.com		Dangerous	No	Shopping	not valid	Yes	Bad	Yes, Not Secured	Yes	Fake
http://airbnb007.netlify.app.prostats.org/	Germany	No	No	Travel	not valid	Yes	Bad	Yes, Not Secured	Yes	Fake
www.airbnb.place-online-search4491911.cc	NA	Dangerous	No	Travel	not valid	Yes	Bad	Yes, Not Secured	No	Fake

ww1.natwesti.com	USA	No	No	Banking	not valid	Yes	Bad	Yes, Not Secured	No	Fake
www.natwestinternational.com	USA	Yes	Yes	Banking	valid	No	Good	Yes, Secured	No	Genuine
http://ww1.barclaya.net/	USA	No	No	Banking	not valid	Yes	Bad	Yes, Not Secured	Yes	Fake
https://home.barclays/	USA	Yes	Yes	Banking	valid	No	Good	Yes, Secured	No	Genuine
http://ww1.lloydstsbs.com/	Europe	No	No	Banking	not valid	Yes	Bad	Yes, Not Secured	Yes	Fake
https://www.lloydsbank.com/	Europe	Yes	Yes	Banking	valid	No	Good	Yes, Secured	No	Genuine
ww1.barclays-supports.com	USA	No	No	Banking	not valid	Yes	Bad	Yes, Not Secured	No	Fake
www.expedia.com	USA	Yes	Yes	Travel	valid	No	Good	Yes, Secured	No	Genuine
www.kayak.com	USA	Yes	Yes	Travel	valid	No	Good	Yes, Secured	No	Genuine
www.cheapoair.com	USA	Yes	Yes	Travel	valid	No	Good	Yes, Secured	No	Genuine
www.yatra.com	India	Yes	Yes	Travel	valid	No	Good	Yes, Secured	No	Genuine
www.makemytrip.com	USA	Yes	Yes	Travel	valid	No	Good	Yes, Secured	No	Genuine

www.cheapoair.com	USA	Yes	Yes	Travel	valid	No	Good	Yes, Secured	No	Genuine
https://www.airbnb.com/	USA	Yes	Yes	Travel	Valid	No	Good	Yes, Secure	No	Genuine
www.holidayinn.com	USA	Yes	Yes	Travel	valid	No	Good	Yes, Secured	No	Genuine

Tool Implementation

This involves how the collected data is analyzed and interpreting data to find the effectiveness of the tool in detecting scams. Examining a tool's effectiveness at spotting and preventing frauds is part of data analysis for a scam detection tool. These are some essential procedures for carrying out a data analysis for a fraud prevention tool. As per the data presentation, here are the steps that I have taken to construct / design a tool. When an URL is entered in my tool, it checks for the IP address. To this I have used *tracert* command line tool where it does validations for both Windows and iOS. Here are the code snippets.



```
// Process traceRt;

String command;

if (os.contains("win")) {

   command = "tracert " + url;

}

else {

   command = "traceroute " + url;

}
```

then looks for the domain name using existing API’s. Then it displays the necessary information on the screen and gives rather good viewpoints for the user to decide on if the website is a valid one or a fake website.

To achieve this, I have used WHOIS API as it does have few limitations and is quite easy to integrate with any of the applications.

```
String uri = "https://ipwho.is/" + ipAddress;
System.out.println("URL is: " + uri);
RestTemplate restTemplate = new RestTemplate();
// WebResult result = restTemplate.getForObject(uri, WebResult.class);
Result result = restTemplate.getForObject(uri, Result.class);
String resp = restTemplate.getForObject(uri, String.class);
System.out.println("Response: " + resp);
// System.out.println("Result: " + result);
return result;
```

The above code shows the implementation of the IP Who API where have used the Rest Template tool to Implement the API call.

For Spell check we have used Google Suggestions API where we get the response as XML format and my tool will read the XML format and gives the results and show user to display 10 spell check suggestion to make sure on their will if they are using a legitimate one or not. Here are my code snippets on how I have used various APIs to make this tool work.

```
String uri =
"https://suggestqueries.google.com/complete/search?output=toolbar&hl=en&q=" + domainName;
System.out.println("URL is: " + uri);
```

```
RestTemplate restTemplate = new RestTemplate();

return restTemplate.getForObject(uri, String.class);
```

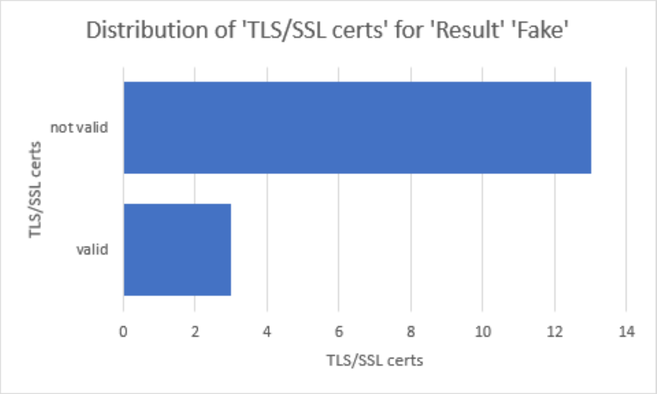
Data Analysis

I will present the results and the analysis of the different websites going through the tool. Using the tool, we have analyzed 32 websites. 16 of them are scam websites and 16 are real websites.

One of the factors analyzed is the website's use of SSL/TLS certificates. In the chart below you can see that in 13 of 16 cases, an invalid SSL certificate is used in case of scam websites. So, this is a good identifier to see if the website used a valid SSL certificate or not. In most cases the fake website can be identified based on the usage of SSL certificates.

Graph 3

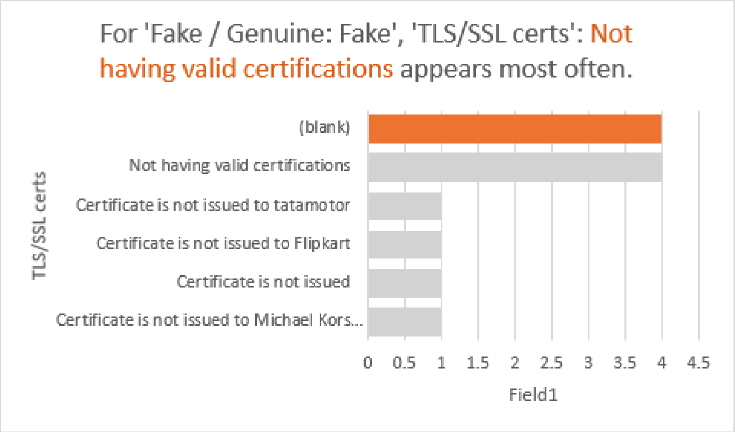
Clustered Bar: Distribution of 'TLS/SSL certs' for 'Result' 'Fake'



I am also showing a breakdown of what a "not valid" fake certificate means in case of fake websites. In most cases, the certificate will not be issued to the organization of the website.

Graph 4

Clustered Bar. For 'Fake / Genuine: Fake', 'TLS/SSL certs'

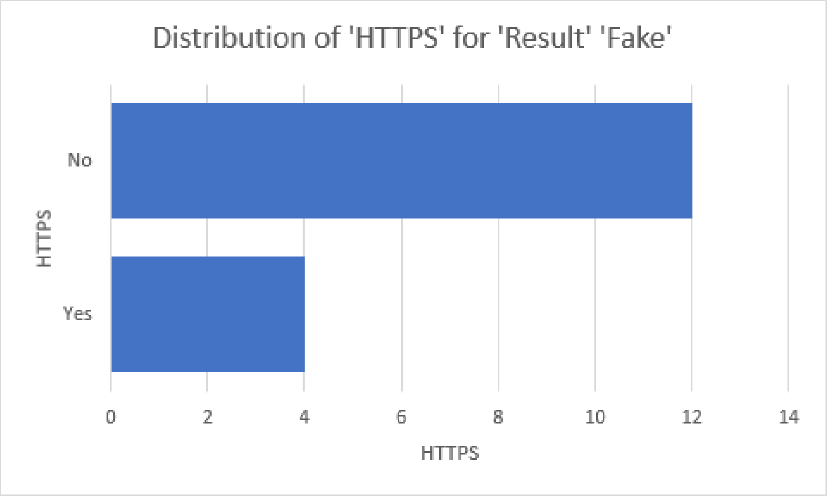


Not having valid certifications appears most often.

Other factor that is analyzed is the use of HTTPS by websites. In the chart below you can see that scam websites use https in less instances. They are used only in 4 out of 16 instances. So, this is a good identifier to see if the website uses secure HTTP protocol.

Graph 5

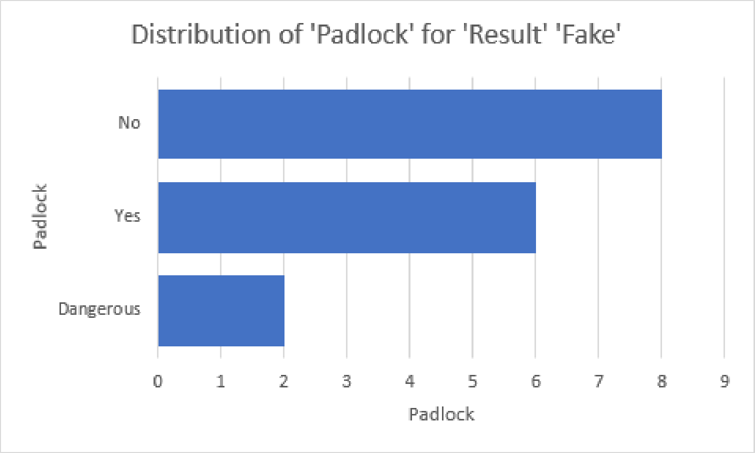
Clustered Bar. Distribution of 'HTTPS' for 'Result' 'Fake'



Another factor we analyzed is the padlock icon that is shown in a browser’s address bar. Typically, having a padlock icon gives the user a sense of safety. Based on the below bar chart, of the 16 fake websites, padlock is not present for 8 websites. In 2 instances, the browser showed a warning “Dangerous” in the place of padlock icon. So, in 50% of instances having a padlock or not having a padlock can help the users avoid fake websites.

Graph 6

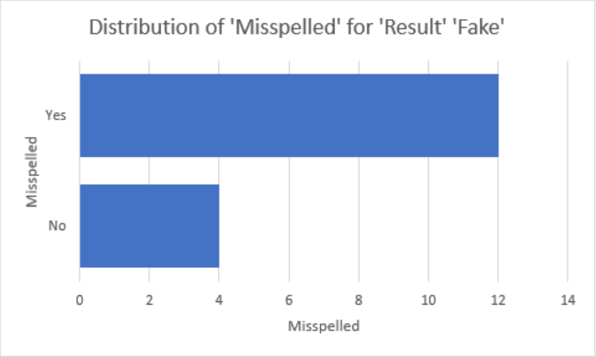
Clustered Bar. Distribution of 'Padlock' for 'Result' 'Fake'



Another factor that we analyzed is fake websites masking their domain name to look like the real website name. We are calling this as misspelled words. Of the 16 fake websites, 12 websites domain names are misspelled. So, this is a particularly good factor to find out if the website is a genuine one or a fake one.

Graph 7

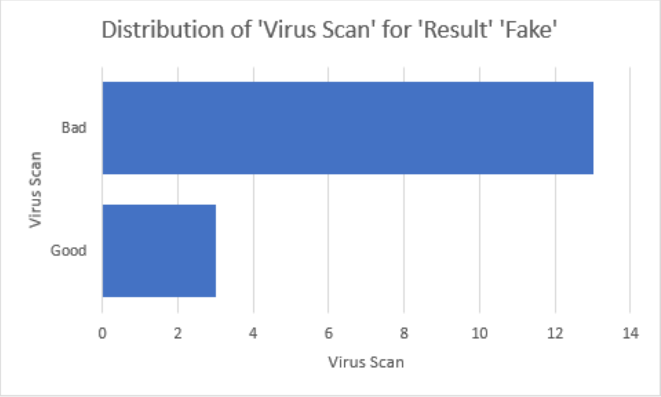
Clustered Bar. Distribution of 'Misspelled' for 'Result' 'Fake'



Another factor analyzed is how an anti-virus software marks a website as fake or genuine. Of the 16 websites, anti-virus software correctly identified 13 websites. Making this factor an important one in identifying a fake website.

Graph 8

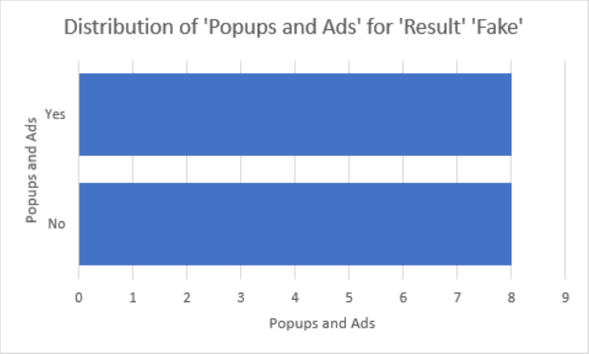
Clustered Bar. Distribution of 'Virus Scan' for 'Result' 'Fake'



Another factor we analyzed is the presence of popup ads. Of the 16 fake websites, the distribution of ads being present is even, with 8 fake websites displaying either popups or ads and the other 8 not displaying them.

Graph 9

Clustered Bar. Distribution of 'Popups and Ads' for 'Result' 'Fake'



Summary

This chapter tells in detail about how the tool works and addresses various API’s that I have used to build. It’s mostly focused on the In Background related to the problem, a detailed description of how I have implemented the tool and tested it with genuine and fake websites. Also analyzed various factors on the results presented in the Tabular form. This chapter also listed some of the data with the code snippets on the design and detailed analysis on the tool in table 2.

Chapter V: Results, Conclusion, and Recommendations

Introduction

In this chapter I am going to present the data collected and analyzed as results in a detailed format. I have also addressed the future scope of the Scam Detection Tool. It also describes how the user should take precautions on entering their personal information in any unknown websites.

Results

Here are the few aspects that have been described below, which are

1. The use of SSL/TLS certificates by the website is one of the aspects examined. According to the table below, an incorrect SSL certificate is used in 13 of 16 occurrences of fraudulent websites. Therefore, this is a reliable indicator of whether the website utilized a genuine SSL certificate. Most of the time, SSL certificates can be used to identify a phony website.

2. The use of HTTPS by websites is another aspect that is to be examined. You can see from the chart below that shady websites employ https less frequently. Only 4 out of 16 situations employ them. Therefore, this is a reliable indicator of whether the website uses the secure HTTP protocol.

3. We also looked at the padlock symbol that appears in the address bar of a browser. The user typically feels safer when they see a padlock icon. 8 of the 16 fictitious websites listed below (seen in the accompanying bar graph) do not have a padlock. The browser's warning "Dangerous" appeared in place of the padlock icon in 2 occasions. Therefore, whether there is a padlock, it can assist consumers avoid fraudulent websites in 50% of cases.

4. Another aspect we looked at was phony websites concealing their domain names to resemble legitimate websites. This is what we refer to as misspelled words. 12 of the bogus websites' 16 domain names contain typos. So, this is a particularly good indicator of whether the website is real or false.

Conclusion

From the above analysis and results presented, most of the fake websites will ask for personal information. When a user enters personal information, he should take all the precautions on checking the secured protocols, Valid website without any misspelled words, look for the padlock symbol on the address bar with http protocol. When a user enters the URL in my tool, it will display the information for the Domain name and suggest some points/thing to look and take care of. Scammers are becoming very intelligent on masking many of the URL’s. When you enter a genuine website URL, they will be directed to another endpoint where the user thinks it’s a genuine one. So, always pay attention while entering any of the personal information and clicking on any of the ad’s that show up on unknown website.

GitHub Link:

https://github.com/SowmyaKaja/spring-petclinic/tree/add-Detect-page

Future Work

The tool depends on extracting the domain name from the input. Every day, scammers are becoming smarter and are using domain names mixed with domain names of famous websites. To extract domains from such complicated structures, we would need advanced logic and Machine Learning. A more readily available tool like a browser addon would make this accessible to more people. The tools could also be expanded to have a cloud DB that can store websites that are tested and websites that are reported or harmful. Users using the tool can be wary if the tool detects a user entered website present in the DB.

Another way to improve the tool is using decision automation, whereas the user types the domain name, the tool should prevent the users from getting the information from the website. When the user wants to know why the tool is preventing from loading the website, the tool should present the reasons to the user with the points which make the website unsafe. The API used to get information about a domain is a free API. Instead of this, if we use a paid version of API, even more information about the domain could be gathered. The browsers help us in getting information about the domain security and its certificate information. This process can also be incorporated into the tool instead of manually looking at the certificate and getting to know about the certificate issued to the organization.

References

3 Airbnb Scams You Need to Know About Before Booking Your Trip. (2021, March 15). MUO. https://www.makeuseof.com/airbnb-scams-to-look-out-for/

5 Uber Scams Everyone Should Be Aware Of. (2020, August 12). Scam Detector. https://www.scam-detector.com/face-to-face-scams/5-uber-scams-everyone-should-be-aware-of

*6 Cruise Scams You Should Never Fall Fo*r. (2019, September 30). SmarterTravel. https://www.smartertravel.com/worst-cruise-scams/

8 Examples of Vishing and How to Beat Them. (n.d.).Terranova Security. Retrieved April 10, 2023, from https://terranovasecurity.com/examples-vishing/

9 Best Anti-Spam Software & Tools For 2021—Fully Reviewed. (2019, July 17). Comparitech. https://www.comparitech.com/net-admin/anti-spam-software/

25 Things About Airbnb Worth Knowing Before Booking. (2018, August 3). TheRichest. https://www.therichest.com/destinations/25-things-about-airbnb-worth-knowing-before-booking/

Abbasi, A., & Chen, H. (2009). A Comparison of Tools for Detecting Fake Websites. *IEEE Computer, 42*, 78–86. https://doi.org/10.1109/MC.2009.306

Airbnb Scams L.A. Out Of $41 Million Each Year, Study Says. (2016, March 31). LAist. https://laist.com/news/a-day-when-theres-only-airbnb

An Introduction to the Different Types of Fraud on the Internet. (n.d.). Kibin. Retrieved November 30, 2021, from https://www.kibin.com/essay-examples/an-introduction-to-the-different-types-of-fraud-on-the-internet-PoS9zy0T

API Documentation | DomainTools. (n.d.). DomainTools | Start Here. Know Now. Retrieved April 9, 2023, from https://www.domaintools.com/resources/api-documentation/

BBB Scam Tracker^{SM}*. (*n.d.). Better Business Bureau. Retrieved December 2, 2021, from https://www.bbb.org/scamtracker/

BBB travel scams websites: Fake travel sites, how to spot 2021. (n.d.). wusa9.com. Retrieved December 2, 2021, from https://www.wusa9.com/article/news/verify/fake-travel-websites-better-business-bureau-fact-check-2021-bbb-travel-scams-latest-list/65-86c0ea58-21bd-4625-b931-ac1bb0f2b9cd

Formplus Blog. (n.d.). *15 Reasons to Choose Quantitative over Qualitative Research.* Retrieved December 15, 2021, from https://www.formpl.us/blog/https//www.formpl.us/blog/quantitative-qualitative-research

Caller ID. (2021). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Caller_ID&oldid=1053751696

ftc—Google Search. (n.d.). Retrieved November 16, 2021, from https://www.google.com/search?q=ftc&oq=FTC&aqs=chrome.0.35i39j46i199i291i433i512j0i433i512l4j0i512j0i433j0i131i433i512j0i512.692j0j9&sourceid=chrome&ie=UTF-8

How To Identify Fake Websites: 11 Warning Signs To Know. (n.d.). Aura (Retrieved April 10, 2023, from https://www.aura.com/learn/how-to-identify-fake-websites

IP Geolocation Documentation. (n.d.). IPWHOIS.Io. Retrieved April 9, 2023, from https://ipwhois.io/documentation

List of Scam websites in 2019 (100% Proved). (n.d.). TrackingMore. Retrieved December 7, 2021, from https://www.trackingmore.com/scam-websites

Newcomer, E. (2017, August 23). *Uber's quarterly losses fall to $645 million as revenue climbs.* San Francisco Chronicle. https://www.sfchronicle.com/business/article/Uber-s-quarterly-losses-fall-to-645-million-as-11953726.php

Papa, A. (2023). *10 Uber Scams You Need to Watch Out For*. Reader's Digest. Retrieved December 7, 2021, from https://www.rd.com/list/uber-scams-you-need-to-watch-out-for/

PhishLabs—The Leader in Digital Risk Protection (n.d.). Intelligence & Mitigation. Retrieved April 10, 2023, from https://www.phishlabs.com/?utm_term=social%20engineering%20attacks&utm_campaign=Social+Engineering+/+Search+/+US%2BEN&utm_source=adwords&utm_medium=ppc&hsa_acc=2617725078&hsa_cam=19324103450&hsa_grp=143889965719&hsa_ad=644413998403&hsa_src=g&hsa_tgt=kwd-381691406863&hsa_kw=social%20engineering%20attacks&hsa_mt=b&hsa_net=adwords&hsa_ver=3&gclid=Cj0KCQjwxMmhBhDJARIsANFGOSsQnWSLuWo7VI-Hzny1jkD-0EJPcc9QcFgy9DsG4GjpUZReSLazVHMaArRDEALw_wcB

Planning a Cruise? Watch Out for These Scams. (n.d.). AARP. Retrieved December 10, 2021, from https://www.aarp.org/money/scams-fraud/info-2019/cruise.html

Rebello, J. (2019, December 10). Over 50% Indians fell prey to discount scams. Tips to stay safe this holiday season. *The Economic Times.* https://economictimes.indiatimes.com/wealth/personal-finance-news/over-50-indians-fell-prey-to-discount-scams-tips-to-stay-safe-this-holiday-season/articleshow/72453319.cms

Report Email Abuse. (n.d.).Southern Adventist University. Retrieved December 10, 2021, from https://www.southern.edu/administration/information-technology/email/report-email-abuse.html

Reuter, D. (n.d.). *Uber is still losing a lot of money.* Business Insider. Retrieved December 13, 2021, from https://www.businessinsider.com/uber-still-losing-a-lot-of-money-latest-earnings-show-2021-8

Scam Website Detector. (2022, November 14). Fake Fraudulent Website Checker. *CWatch Blog.* https://cwatch.comodo.com/blog/website-security/how-to-spot-a-fake-fraudulent-or-scam-website/

Scam websites: How to identify fake sites. (2023, March 8). NordVPN. https://nordvpn.com/blog/fake-scam-websites/

Schlappig, B. (2019, December 7). *Help Me Understand The Uber Cancelation Scam?* One Mile at a Time. https://onemileatatime.com/uber-scam/

Snapshot. (n.d.). Domain Tools. Retrieved April 9, 2023, from https://www.domaintools.com/resources/api-documentation/whois-history/

Spamfighter tool—Google Search. (n.d.). Retrieved December 15, 2021, from https://www.google.com/search?q=spamfighter+tool&sxsrf=AOaemvIMotPCLKTPGwcxSGYH9KCzW4TbFQ:1639600894273&source=lnms&tbm=isch&sa=X&ve

d=2ahUKEwiik4Gn1eb0AhVJjYkEHUKgDeMQ_AUoAnoECAEQBA&biw=1280&bih=577&dpr=2.5#imgrc=Pt_4RgatkKBRlM

This Driver in China Explains How He Is Helping Rip Off Uber. (2015, June 28). Bloomberg.Com. https://www.bloomberg.com/news/articles/2015-06-28/this-driver-in-china-explains-how-he-is-helping-rip-off-uber

Threat Trends Report: Crypto Malware, Phishing, Trojans and more. (n.d.). Cisco Umbrella. Retrieved April 10, 2023, from https://umbrella.cisco.com/info/threat-trends-report-cryptomining-malware-phishing-trojans?utm_medium=search-paid&utm_source=google&utm_campaign=UMB_23Q3_NA_EN_GS_Nonbrand_Threats&utm_content=UMB-FY21-Q4-content-ebook-2021-cyber-security-threat-trends&_bt=617192065197&_bk=phishing+in+cyber+security&_bm=e&_bn=g&_bg=122023014712&gclid=Cj0KCQjwxMmhBhDJARIsANFGOSt_aWlhBuGnGaRXFxM_MtRV_OHlZzqWfFMtkLF09vhd10nt3M58cboaAniYEALw_wcB

Travel scams up 4x as pandemic recedes and travelers take flight. (2021a, June 30). *Bolster Blog.* https://bolster.ai/blog/travel-scams-up-4x-as-pandemic-recedes-and-travelers-take-flight/

Travel insurance: ABI. (2021). Association of British Insurers. https://www.abi.org.uk/products-and-issues/choosing-the-right-insurance/travel-guide/

TSA checkpoint travel numbers (current year versus prior year(s)/same weekday). (n.d.). Transportation Security Administration. Retrieved June 1, 2023, from https://www.tsa.gov/travel/passenger-volumes

Watson, S. (n.d.). *Preventing and detecting travel insurance fraud.* ITIJ. Retrieved December 11, 2021, from https://www.itij.com/latest/long-read/preventing-and-detecting-travel-insurance-fraud

What is a Cloudmark fingerprint and how does it work? (n.d.). Validity Help Center. Retrieved December 14, 2021, from https://help.returnpath.com/hc/en-us/articles/220564147-What-is-a-Cloudmark-fingerprint-and-how-does-it-work-

What Is a Malware Attack? Definition & Best Practices. (n.d.). Rapid7Retrieved April 10, 2023, from https://www.rapid7.com/fundamentals/malware-attacks/

What is Traceroute? How It Works and How to Read Results. (n.d.). Retrieved April 9, 2023, from https://www.varonis.com/blog/what-is-traceroute

Which Nations Are on the UK Government's Safe Travel List?. (n.d.).GoCompare. Retrieved December 11, 2021, from https://www.gocompare.com/travel/uk-safe-travel-list/

Whois History. (n.d.). DomainTools. Retrieved April 9, 2023, from https://www.domaintools.com/resources/api-documentation/whois-history/

Wilson, D. (2021, June 15). *Nearly $75M lost to vacation scams since start of COVID-19 pandemic.* ABC11 Raleigh-Durham. https://abc11.com/10789440/

With the Return of Travel Comes the Return of Robocall Travel Scams. (n.d.). Frommer's. Retrieved December 12, 2021, from https://www.frommers.com/blogs/arthur-frommer-online/blog_posts/with-the-return-of-travel-comes-the-return-of-robocall-travel-scams

Ychin. (n.d.). *Understanding SpoofGuard.* Retrieved December 13, 2021, from https://docs.vmware.com/en/VMware-NSX-T-Data-

Center/2.3/com.vmware.nsxt.admin.doc/GUID-2E331082-1D1C-4B51-BB5A-A909BCD5FED0.html

Zhang, Y., Wu, Q., Zhang, T., & Yang, L. (2022, November 28*).* Vulnerability and fraud: Evidence from the COVID-19 pandemic. *Humanities and Social Sciences Communications, 9,* 424. https://www.nature.com/articles/s41599-022-01445-5