IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.88110

PHISHING IN INDIA – ANALYTICAL STUDY

Dr. Anusuya Yadav[1]

[1]Assistant Professor, Law Department, MDU Rohtak, Haryana, India

ABSTRACT: The increasing use of the internet coupled with almost perpetual digital illiteracy has given an upsurge to increasing cybercrimes. These Cybercrimes include extortions like ransomware, online frauds like phishing, exploitations like hacking, and much more. Amongst these, Phishing has been making an enormous impact on data privacy over the past two decades. Phishing falls under Social Engineering Attacks. In phishing, the confidential data of an individual, group, or organization is obtained through online fraud. When an individual or a group, commonly known as a hacker(s) stealsconfidential information by claiming to be a genuine organization, individual, or group, then it is called phishing. In comparison to other cybercrimes,Phishing can be done with ease, and it also decoys more users to disclose sensitive information. This paper describesan analysis of Phishing Attacks in India. And some redolent methods to spread awareness about phishing.

Keywords: Phishing, Fraud, Attacker, Cybercrime, Cybercriminals.

1. INTRODUCTION

Cybersecurity has always been a big concern. There has never been a time when cybersecurity researchers have overtaken cybercriminals because cybercriminals have to find only a small loophole to sabotage the entire cybersecurity infrastructure. This can be gauged from the fact that last year, hackers placed their payload into the Orion product of the SolarWinds company and they stole the information without being detected for a long time, until about a year later, when the cybersecurity Company FireEye reported it, around 30000customers of the SolarWinds were infected [1]. Of these, more than 18000 are government and private users.

Not only this, but digital illiteracy is also a big purposebehind increasing cyber-crimes.As claimed by DEF India's 2018 report, nearly 90% of India's people were digitally illiterate [2]. Obviously, digital literacy would have been increased, but so do the number of internet users.Today, from the age of 5 years old to the old age of 90, everyone uses the Internet, and among the children, a different status has been formed regarding the use of the smartphone. Today every child insists on getting a smartphone and at the same time, they get the facility of the internet. Similarly, whether anyone knows how to use the Internet or not, everyone is busy in using the Internet [3]. People unknowingly often give access to such things, which should not be given access. According to Google, 50% of mobile ad clicks are made by mistake and 72% of these redirects to malicious sites [4]. Which are very popular for online fraud.

According to Google, since the coronavirus pandemic started, phishing sites have increased by 350%[5]. By taking advantage of digital illiteracy, cybercriminals are luring people to easily extract sensitive information from them. Not only websites but also email and telephone are being used for phishing. Cybercriminals are getting information from people by pretending to be legitimate authorities. Every year Google blocks thousands of phishing sites but they are increasing. Web Browsers use many such algorithms that easily detect phishing and warn the user, but still, there are many websites on which phishing is done on a very large scale.The image present below shows the warning what Microsoft Edge shows when a phishing URL is detected.

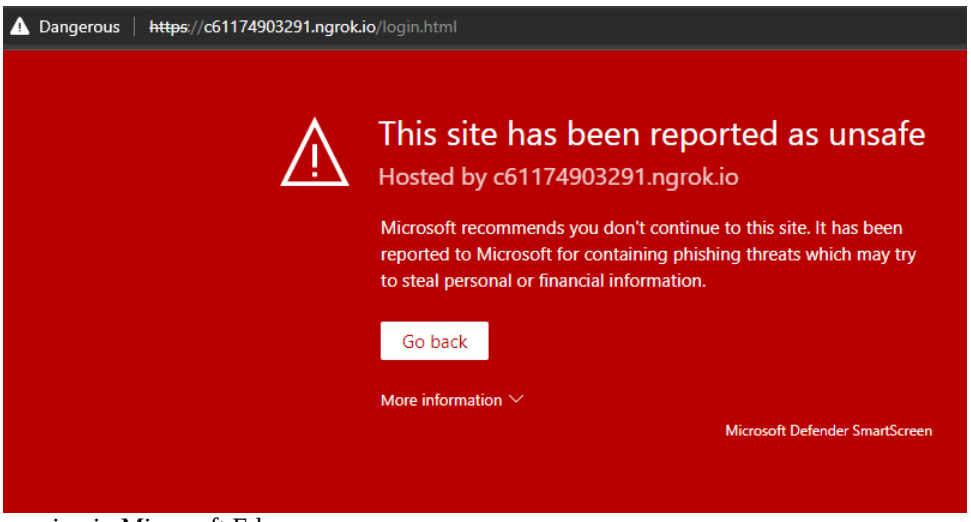
IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

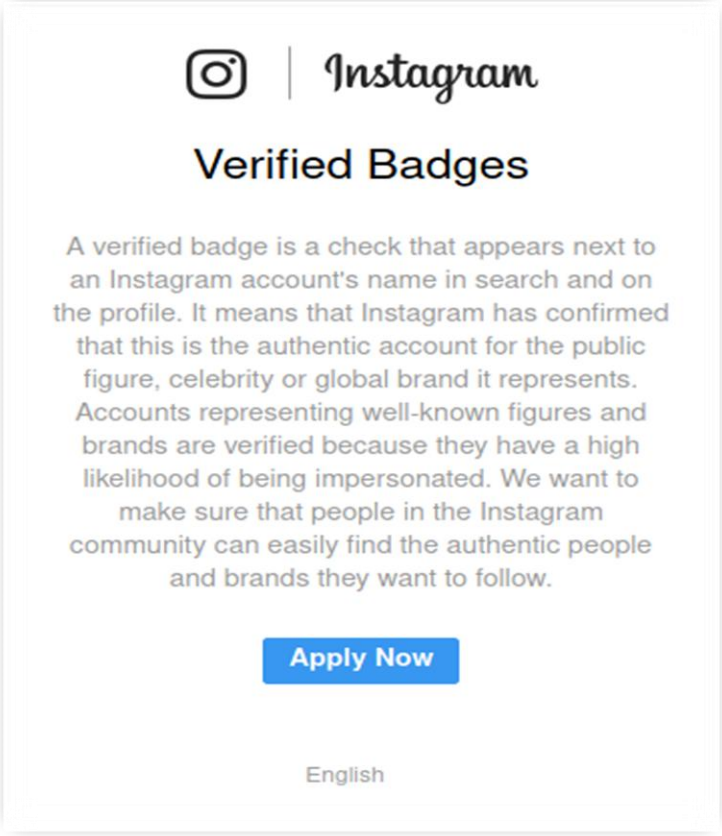
Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.88110



Phishing URL warning in Microsoft Edge

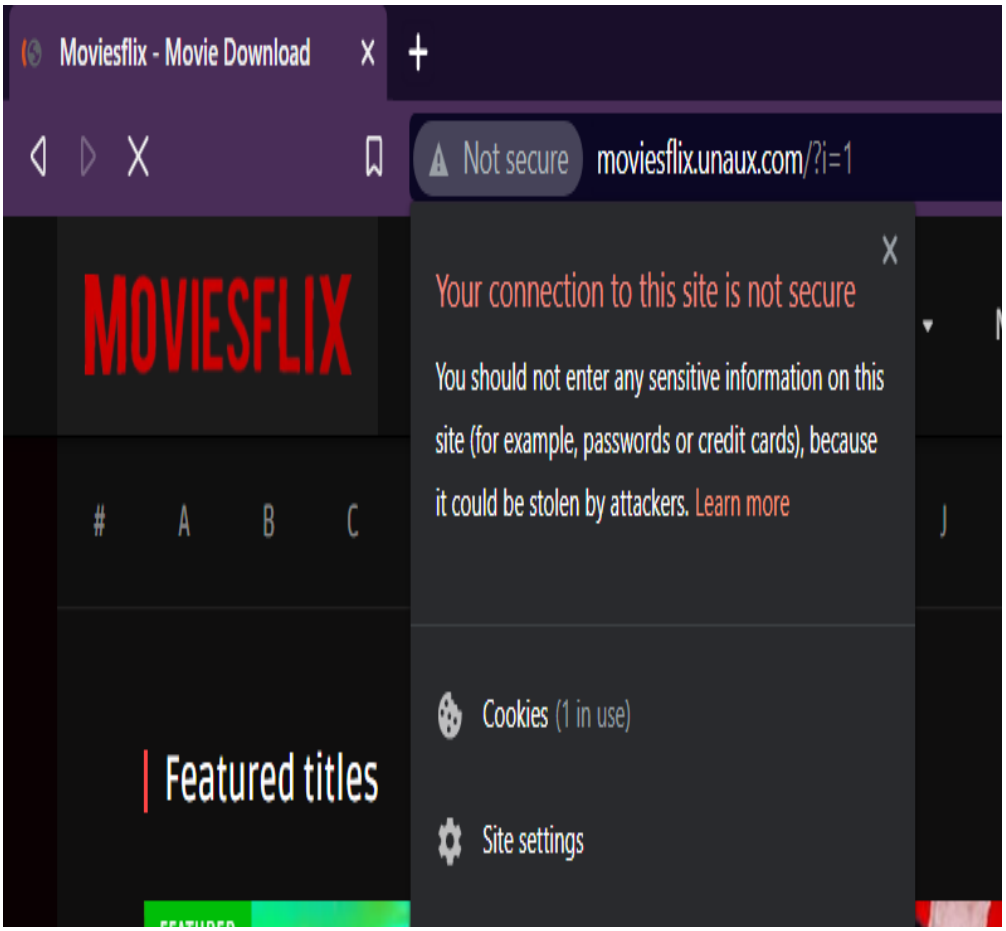
Usually, people are tempted by making fake links, such as expensive products are being sold cheaply on Amazon, some big brandsaregiving 99% discounts, paid services are available for free, or by intimidating people, the details are taken. These intimidating emails often contain messages like expiry of password, or service, etc. The image shows belowcontains a phishing template of Instagram luring users to have verified badges on the accounts.



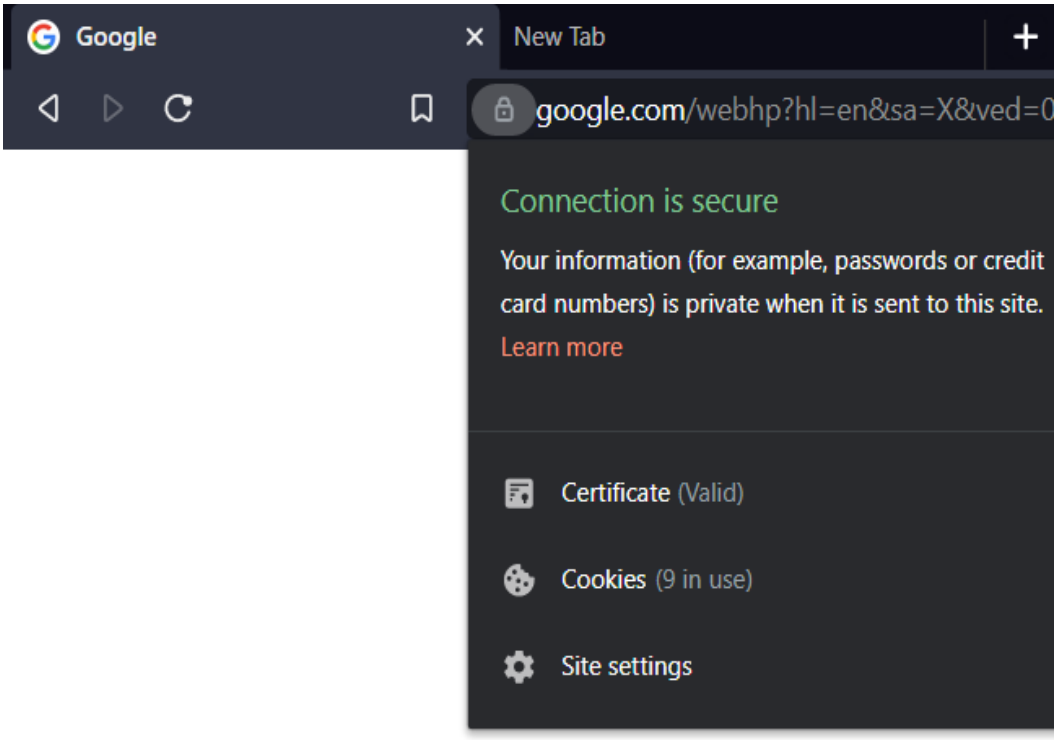
Phishing Template of Instagram generated by tool zphisher.

Address bar where the URL of the website is displayed, we should pay attention to it while visiting any unknown website, and should also pay attention to the digital certificate.But usually, it is not done. When we go to a legitimate website, we get to see a lock icon in the address bar, if we click on that icon, then we can see its digital certificate, but if the website is fake, then instead of the lock, a warning symbol appears. So, by looking at the address bar, we can check the authenticity of a website. The images shown below represent the difference between a legitimate website and a fake website.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 8, August 2021
DOI: 10.17148/IARJSET.2021.88110



A non-secure website (http://moviesflix.unaux.com).



A secure Website(https://www.google.com/)

Despite all the protective methods being used, phishing is top-notch and is constantly making more victims.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 8, August 2021
DOI: 10.17148/IARJSET.2021.88110

2. TYPES OF PHISHING

Phishing has spread afar e-mail to include VOIP (Voice over Internet Protocol), SMS (Short Message Service), instant messaging services, social media networking sites, even multiplayer games, and other online platforms. Though Phishing can be categorized into various types, below are some major types of Phishing [6]. Figure1 shows the various types of Phishing Attacks.

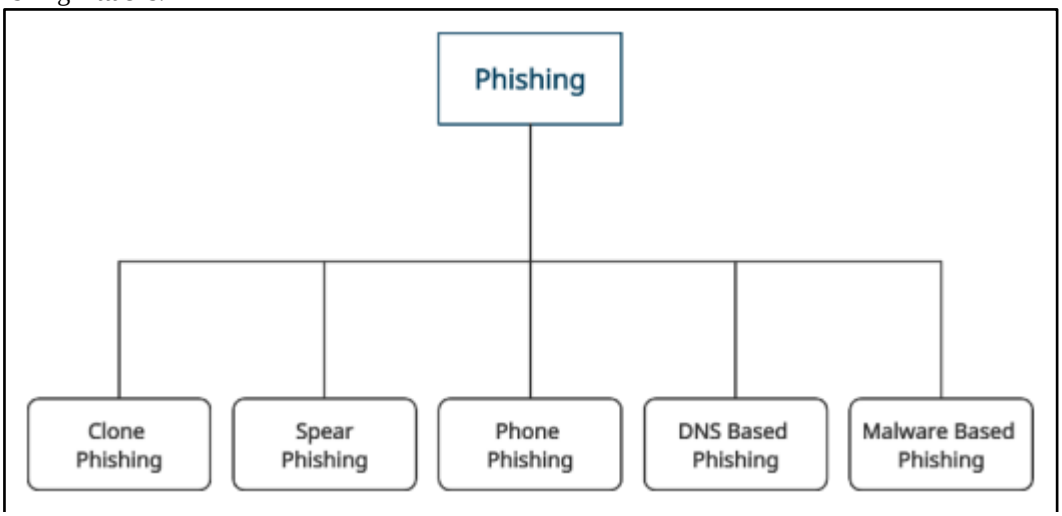


Fig1: Types of Phishing Attacks.

- **Clone Phishing:** It is a type of Phishing where the attacker tries to make a clone of a website that is often visited by the users. Most of the cloned websites are banking or other fund transferring websites. These cloned websites most often ask for login credentials. Whenever the user provides the login credentials, the users are authenticated to the real websites, while the login credentials of the user get stored in the database of the cloned website. These URLs of cloned websites are delivered to the users through emails, text messages, and sometimes through popup windows in web browsers, alerting users that their passwords are going to expire [6]. These URLs are sent to a lot of random users.
- **Spear Phishing:**Spear phishing refers to sending emails to a group of people while claiming to be a legitimate sender. So rather than sending emails randomly, selected groups of people with something in common are targeted. The aim of the attackers is to either exploit devices or to convince victims handy over information or money. Phishing attacks began when the Nigerian prince scammed in the mid-1990s, today they have to be mutated into well-researched and targeted operations that are both highly effective and exceptionally challenging to stopover.
- **Phone Phishing:**In phone phishing, attackers make calls to multiple users by pretending to be an authorized service provider such as a bank customer service agent, or an insurance policy agent, etc. They capture users in their sweet talk and try to gather as much information as possible, usually, the targets are either older people or illiterate people. A similar view can be seen in Airtel's Safe Pay advertisement.
- **DNS-Based Phishing:** When a user visits a website, a DNS server converts the domain name to some IP address, but if the website's DNS records or DNS servers are exploited somehow, the traffic may be routed to a malicious website that attracts users to either download something malicious or to provide sensitive information. In pharming, the DNS records of a website or DNS server are corrupted by the attackers, and hence they divert the incoming traffic to a legitimate website, and thereby they do phish with the help of their malicious websites.
- **Malware Based:**In malware-based phishing, an attachment is added with the phishing email. This attachment can be anything a document, picture, or other media embedded with some malicious code, maybe a virus, worm, or other malware. Usually, this embedded code is ransomware, like in the case of WannaCry**.**

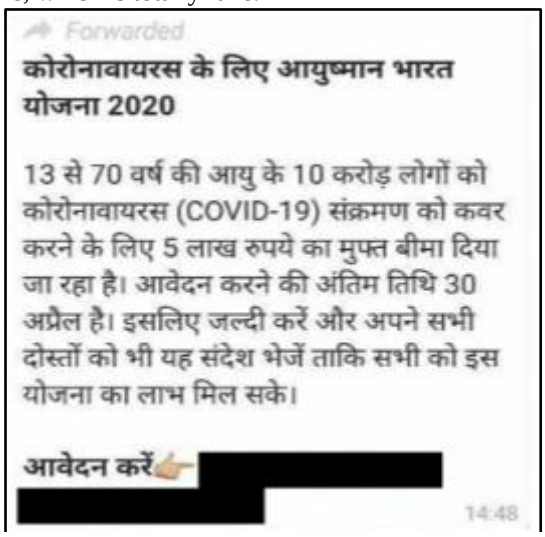
3. ANALYTICAL STUDY

When we talk about scams and frauds, India no longer sits back. In the past two decades, there have been major online scams like the freedom 251 mobile scam of 2016, OLX scams, online discount scams, etc. Generally, Online transfers are the biggest drawbacks of scams like the online selling of items. Nowadays the intermediary or you can say broker-type websites and apps like OLX or quicker has become the main platforms of online frauds. These show some immovable properties at extremely low prices or movable properties like LCD or LED TV Cameras at very low prices[7]. The irony of these advertisements is that the location of the seller is shown in the local region, whereas in reality, they are not. Sellers are very remotely based. When contact is made to the sellers they claim to be busy professionals working a thousand kilometers away. If we contact them to buy some items, then they will ask to transfer

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 8, Issue 8, August 2021
DOI: 10.17148/IARJSET.2021.88110

money to their account as an advance. Some people fall into their trap in the greed of buying things at cheaper rates. And that's how the whole selling scam is operated. It's not the only one type of scam practiced in India.

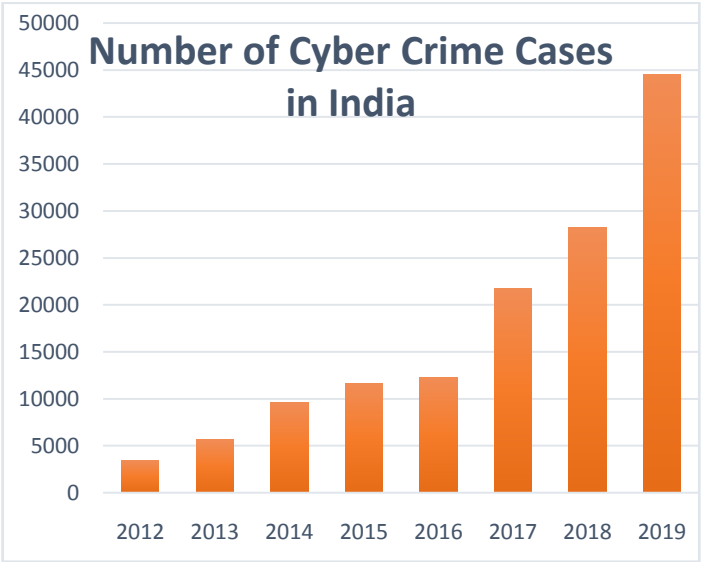
During the COVID-19 times, there was a sudden increase in the number of scams, scammers taking great advantage of the pandemic. Scammers came up with many fake schemes in the name of the Indian or State Government, and many people got trapped in these fake schemes. And the work of pouring petrol into the fire is done through social media, where people keep forwarding things without thinking. We often see that whenever we get a message of such a fake scheme on WhatsApp, it is written on it "Forwarded many times", from this we can estimate that through how many people this fake message must have come to us.The image given below shows a message circulated over WhatsApp about an Indian Government Scheme, which is totally fake.



A fake message about a fake scheme
(Source: https://www.businessinsider.in/)

Social media giants like WhatsApp, try hard so that fake news and fake messages don't circulate. People are also informed through various advertisements, but there is not much difference. And this is because of digital literacy. But until people do not understand their role in circulating fake things, nothing can happen.

The below-mentioned data shows the increasing trend of cyber-crime in India[7].



Source: https://www.statista.com/statistics/309435/india-cyber-crime-it-act/

These figures clearly show that within seven years the crime reported increased more than 10 times. From 3477 cybercrime cases in 2012 to 44,546 cybercrime cases in 2019, there is a humongous increase. Even the digits got almost doubled within a year from 27,248 cases in 2018 to 44,546 in 2019. This clearly shows that in 2019 a drastic jump is analyzed in cybercrime cases over 44.5 thousand cases were registered that year[7].

IARJSET

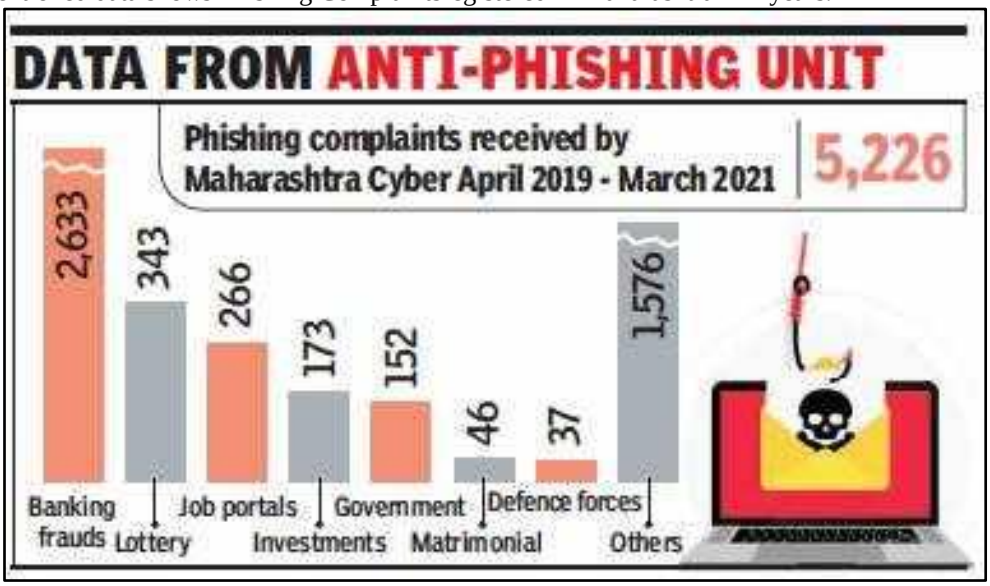
ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Vol. 8, Issue 8, August 2021

DOI: 10.17148/IARJSET.2021.88110

The below-mentioned data shows Phishing Complaintsregistered in Maharashtra in 2 years.



(Source: https://timesofindia.indiatimes.com/)

This clearly shows that Major frauds are related to the baking sector. RBI stated that banking sector frauds in the year 2019-20 were around 2 lakh crores.In the year 2019 in cyber roads, Maharashtra ranked 1 followed by Bihar. These were the two States with around 5000 cyber fraud cases [9].

CONCLUSION

Phishing attacks are among the major cyber-attacks that take place in India. Phishing is a practice to collect sensitive information by luring people. Phishing is one of the most treacherous cyber-attacks that take place in organizations, personal devices, etc. The criminals who carry out these attacks are hard to catch. This is due to many inexperienced and unsophisticated users. Though technologies are advancing for phishing detection, but users also have to take some awareness to protect themselves. Whenever there is an email or any message from an unknown sender, do not react to it, checking the URL before entering your personal details on any website, if theURL is suspected then don'tuse the site, while doing something on any website checking the digital certificate, not forwarding the message without verifying, all these are some of the ways to keep yourself and others safe.This study shows clearly that Phishing is an easy method of stealing someone's information due to their lack of awareness. This study may give the awareness about the problems that cause phishing and the solutions to phishing attacks that is one of the biggest threats to digital information.

REFERENCES

1. Oladimeji, S. S. M. K. (2021, June 16). SolarWinds hack explained: Everything you need to know. WhatIs.Com. https://whatis.techtarget.com/feature/SolarWinds-hack-explained-Everything-you-need-to-know
2. Srivastava, S. (2020, September 8). International Literacy Day: Bridging India's Digital Divide. BloombergQuint. https://www.bloombergquint.com/technology/international-literacy-day-bridging-indias-digitalivide#:%7E:text=As%20per%20a%20report%20from,India's%20population%20is%20digitally%20illiterate.&text=The%20coverage%20targets%20have%20been,in%20rural%20India%20digitally%20literate.
3. D.A.Y. (2020, December 18). Cyber Security: The Emerging Need of India. Wesleyan Journal of Research, 13.
4. Team—Dcn, R. (2016, February 11). Sixty percent of mobile banner clicks are accidental. Digital Content Next. https://digitalcontentnext.org/blog/2016/02/10/sixty-percent-of-mobile-banner-clicks-are-accidental/
5. Damiani, J. (2020, March 26). Google Data Reveals 350% Surge In Phishing Websites During Coronavirus Pandemic. Forbes. https://www.forbes.com/sites/jessedamiani/2020/03/26/google-data-reveals-350-surge-in-phishing-websites-during-coronavirus-pandemic/?sh=45f4cbac19d5
6. D.A.Y. (2021). PHISHING ATTACKS IN INDIA: ISSUES AND CHALLENGES. Sambodhi (UGC Care Journal), 44(1), 27–31.
7. Dr. Anusuya Yadav. (2021). Cyber-Crime: A Study of Gurugram and Rohtak Districts. International Journal of Modern Agriculture, 10(1), 942 - 948. Retrieved from http://www.modern-journals.com/index.php/ijma/article/view/696
8. Joshi, M. C. A. (2019, May 23). Phishing in India is becoming innovative. Indiaforensic. https://indiaforensic.com/understanding-phishing-india/
9. Shubhangi Taneja; Ruchi Pal; Shiwangi Vishwakarma; Rakesh Kumar. "A Case Study on Cyber bullying". *International Research Journal on Advanced Science Hub*, 2, 7, 2020, 29-31. doi: 10.47392/irjash.2020.60

