IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁙ Impact Factor 8.102 ⁙ Vol. 12, Issue 3, March 2023

DOI: 10.17148/IJARCCE.2023.12368

# Phishing Attack

**Rupali.S.Shinde[1], Komal.S.Kamble[2], Sakshi.G.Shende[3], Mrs. Swati Patil[4]**

Student, Computer Technology, Bharati Vidyapeeth Institute of Technology, Kharghar, India[1-3]

Guide, Computer Technology, Bharati Vidyapeeth Institute of Technology, Kharghar, India[4]

**Abstract**: In the world, internet users' numbers are increasing at the same time cybercrime is also increasing. Now, these days cyber-attack rate is high. There are various types of cybercrime. Steal the victim's personal information like a username, password, credit details, users' sensitive data, personal information, etc. Attacks by phishing emails, phishing messages, phishing URLs, and websites are the popular ways of the phishing attack. Social media and online gaming popularity increasing nowadays attackers are targeting these platforms for phishing- attacks.

**Keywords:** Cybercrime, Hacker, Target, Attack

## I. INTRODUCTION

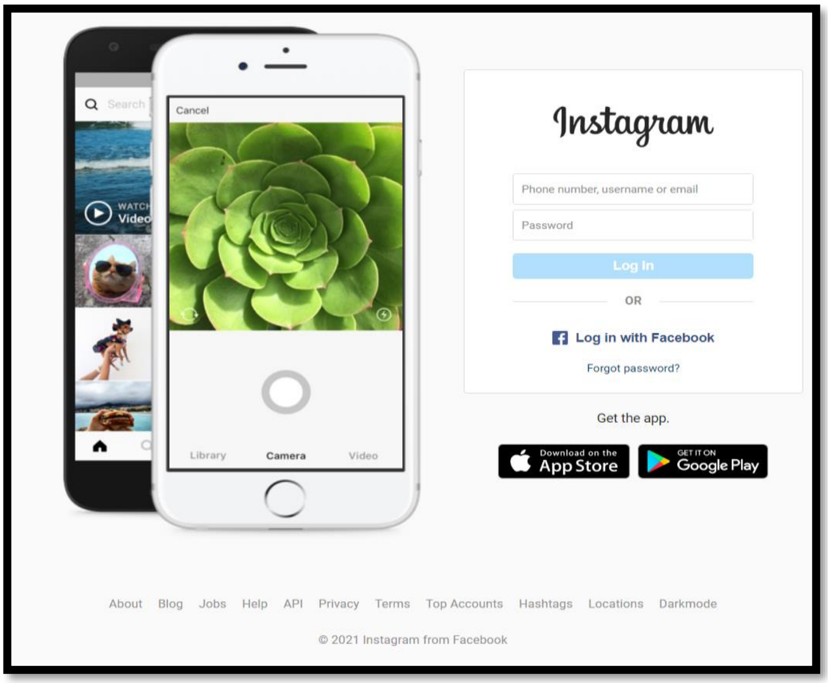
The phishing attack is a way of hacking. Usually, it is done through SMS or email. The phishing attack is used to steal anybody's sensitive information i.e., password, bank details, social media, and login information. Install malware in the target's machine. In a phishing attack, an attacker uses a trick to hack any machine. There is the most common type of phishing attacks: 1) Email phishing 2) Spear phishing 3) Smishing and vishing 4) Whaling 5) Angler phishing. Because of lack of security awareness phishing attacks are done. For phishing first step is building a fake or spoof website and then sending that website to the target. After sending the website collect the victim's all information. In India, the phishing case is Panjab National Bank Scam. To save ourselves from phishing attacks, we should use antivirus and never share our details with anybody.

## II. LITERATURE SURVEY

The attacker sends a fraud massage ( e.g., fake, deceptive, or spoofed ) for getting the target's sensitive information it is called a phishing attack and it is a type of social engineering[1]. Like ransomware on the weak team's infrastructure to deploy malicious software. Phishing attacks often transparently mirror the site being targeted and it is increasingly sophisticated, while the victim is navigating the site it allows the attacker to observe everything, and transverse any additional security boundaries with the victim[2]. Phishing is the most common attack performed by cybercriminals, with the center recording over twice as many incidents of the FBL internet crime complaint than any other computer crime[3]. Some kinds of social engineering are involved in most types of phishing in which victims are psychologically manipulated into acting like clicking on the link, opening, and attaching, disclose confidential information. The entity, the creation of a sense of urgency attackers claims that user accounts will be shut down unless the victim takes an action to involve in most phishing [4]. It occurs most often with target bank or insurance accounts[5]. By email spam most phishing mass messages delivered and it is not targeted are by the personalized specific company – it is termed "bulk" phishing [6]. The fast internet connectivity smartphone is now saturated, sending email malicious links can yield the same result as it would if sent via SMS in a strange or unexpected format the telephone numbers may get smishing messages [7].
Smishing attacks usually invite the user to call a phone number or contact or email address provided by the attacker via an SMS or click a link . the target is invited to provide their private data often, credentials to other services or websites . as well, due to the URLs may not be fully displayed, nature of mobile browsers it makes more complicated to identify an illegal login page [8].

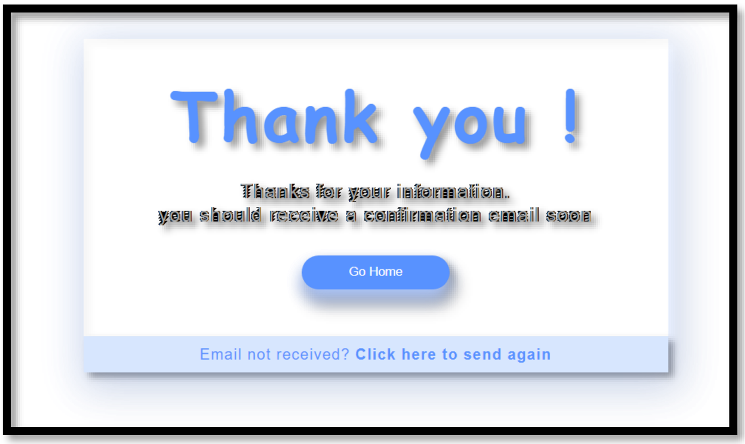
## III. PROPOSED SYSTEM

**a. Fake Message:**
Firstly, the hackers send links or messages to the target. To make the user fool and get the information.
**b. Homepage:**
When the user clicks the link the homepage of the project is open. For the first operation, the user needs to enter an account or login (sensitive data) there.



**3. Database:**
In the database when the user enters the data or logs in. At that time all the data is stored in the database which is running in the background of the project.

**4. Thank you Page:**
The user logs in to the page that time displays the thank you message on the user's screen. To pretend that log is successful.


Thank you !

Thanks for your information.
you should receive a confirmation email soon

## IV. SOFTWARE REQUIRED

1. HTML
2. CSS
3. Database
4. Node js

## V. MERITS

- You will be able to get all the details of the users.
- Easy to use.
- Well-fair scheme.
- Intelligence department.
- Monitoring elements.

DOI: 10.17148/IJARCCE.2023.12368

## VI. Demerits

- If the user changes the password, it will automatically log out.
- The link can also use for the wrong purpose.
-

## VII. Future Scope

Future phishing attacks may take a variety of shapes and become unrecognisable. We will break into the other application with the aid of a phishing assault. for the correct reason. Enterprises currently require phishing protection. like email security to stop phishing attempts. Additionally, SIEM solutions include user and entity behaviour analysis (UEBA), a feature that can assist in identifying hackers who impersonate legitimate users by stealing their credentials.

## VIII. Conclusion

We are going to do this project through social engineering. With this project, we will get users' information. This project "Phishing Attack" is developed using HTML, CSS as the front end, and Node js, database in the backend. In this project, we also show how phishing attack works.

## References

[1]. Jansson, K.; von Solms, R. (2011-11-09). "Phishing for phishing awareness". Behavior & Information Technology. 32 (6): 584–593. doi:10.1080/0144929X.2011.632650. ISSN 0144-929X. S2CID 5472217.

[2]. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark; Stavroulakis, Peter (eds.). Handbook of Information and Communication Security. Springer. ISBN 978-3-642-04117-4.

[3]. "Internet Crime Report 2020" (PDF). FBI Internet Crime Complaint Centre. U.S. Federal Bureau of Investigation. Retrieved 21 March 2021.

[4]. Cui, Xinyue; Ge, Yan; Qu, Weina; Zhang, Kan (2020). "Effects of Recipient Information and Urgency Cues on Phishing Detection". HCI International 2020 - Posters. Communications in Computer and Information Science. 1226: 520–525. doi:10.1007/978-3-030-50732-9_67. ISBN 978-3-030-50731-2. S2CID 220523895.

[5]. a b Williams, Emma J; Joinson, Adam N (2020-01-01). "Developing a measure of information seeking about phishing". Journal of Cybersecurity. 6 (1). doi:10.1093/cybsec/tyaa001. ISSN 2057-2085.

[6]. "2019 Data Breach Investigations Report" (PDF). PhishingBox. Verizon Communications. Retrieved 21 March 2021.

[7]. "What is Smishing?". Symantec Corporation. Retrieved 18 October 2018.

[8]. Mishra, Sandhya; Soni, Devpriya (August 2019). "SMS Phishing and Mitigation Approaches". 2019 Twelfth International Conference on Contemporary Computing (IC3). IEEE: 1–5. doi:10.1109/ic3.2019.8844920. ISBN 978-1-7281-3591-5. S2CID 202700726.