Review Article

Best Plan to Protect Against Phone Phishing Attack

GAURAV KUMAR*

Dep. Of Information Technology,
Bengal College Of Engineering & Technology,
Durgapur, West Bengal, India

***Corresponding Email:** kgaurav226@gmail.com*

ABSTRACT

Phishing is major issue in the world as well as in the internet world and it seen that some case of phishing attack is done by phone. Now these days whole world are suffering to the phishing and case of phishing are increase suddenly days to days, many of Anti phishing organization work on to protect user or people to the phishing attack but there rate of percentage of success are less and rate of phishing are suddenly increases. In this present work first I write concept of phishing and phone phishing to understand the term phishing and proposed plan to protect against phone phishing mainly to the phone fraud, if we work start on the plan or start practical work on the proposed plan we can easily say that we are safe from phone phishing attack, experimental result in this work show that the method work successfully or safe to the phone phishing attack.

Keywords: Phishing, Phone Phishing attack, Phone Phishing technique.

INTRODUCTION

Phishing is fraud method in which the attacker accrues sensitive information or financial information likes credit card, user name, password details sometime money also[1,12]. Commonly the messages appear to come trustworthy, well known and famous websites. Websites that are widely used by phishers in purpose of spoofed like eBay, PayPal, Yahoo etc and now this day phishing keep growing[2]. The risk of grows in larger in the social media likes Facebook, Google+ and Twitter[3]. Phishers take help of these trustworthy and famous websites to attack on people using them on their home, workplace to take security such as personal information which can be affect organization. Generally Security refers the safe of your data in the terms of security to the phishing the data are credit card, user name and password or security information[4]. In the common word phishing is the more often example of social engineering technique used by device user[5]. Now this days Phishing are growing rapidly in worldwide, the Phishing case are increasing year by year more suddenly and many Organization such as government, private work on the

Protect user or public against the phishing.

Phone Phishing technique is now these days widely used by phishers to spoofing people. Phone phishing is criminal work of using the social engineering work often the telephone or mobile phone to gain private access and financial access of people to phisher's financial profit. The mission of Anti phishing working organization or group is provide a resource for information such as phishing attack problem such as solution of problem for phishing or email fraud[6.]

OVERVIEW

A. PHONE PHISHING

Phone phishing are criminal activity using the social engineering service often the use of telephone or mobile phone to accrue the sensitive or private information to make phishing financial profit. Phone phishing are widely increased in this day. In this type of phone phishing attacker message you that you win some amount of money and if you interested to claim the money send your security or personal information likes name, mobile number, address, account number etc. One another type of phone phishing is also target by phishers that are directly they call you and give you phishers own details of name higher bank authority and tell you about wrong or fake issue of your account and request you to give your sensitive information or security information likes credit card details likes number, pin, cvv number of credit card etc. The phone phishing techniques are suddenly increased in now in this era. Some time they call you and told you I am taking with the Higher bank authority and talking about your account are blocked provide me details to reopen the account but in the actuality they are try to target you for phishing or attack and in this type of phone phishing sometime they also message you with the help of Internet.

1. Sign of a phishing

In this basically the scammers or phishers don't give you time to think about own intention just call you and start own pre minded thinks such as targeting you and talk with you some like that I am higher level authority of financial organization and your account are blocked if you reopen them I need to some verification but in reality they

Targeting you, another one is call you and tell you that you are specially selected for the prize or the offer or you are won our five valuable prize or you are selected for a big amount of prize of foreign country etc like that[9.]

2. How they hook you

In sometimes use of fake prize, offers, product or services as bait but some of their use mail, text or ads to get you call them for your valuable details in such manner they targeted you. In some of case they give you offer like that low cost travel package or free cost travel package in the coming vacation and the advance fees loans, credit card protection sometimes free trail offers such as sign up and get free product in the some case they also uses name of charitable trust also they told you some like that urgent request for charitable relief like that , one of the famous method of the scammers are uses name of foreign lottery actually these pitches are against the law which uses cross border sale of lottery ticket with the help of phone or mail in actually you never see a ticket but the main purpose scammers intention are targeting you such as information they take these method there are several different technique for the use for hooking a people[9.]

3. Why they call you

The fraud is not limited in race such as ethnic background age, gender and education. Sometimes it seen that scams seems to concrete in certain group and sometimes scammers are target the old people because they live alone and the scammers think like that the old people are more polarized to the scammers and the chance of success become high [9].

4. What to do about prerecorded call

Sometimes it's seen that the scammers call the help of prerecorded voice and after call the tell you about selling product and some like that if you try to buy talk with the our live operator or press one or any other number to talk with the our live operator generally in often word it's called robocall and when you press any keyword then the scammers secure you are going on their sense and then phone call operated by directly scammers and he try to take your sensitive such as private information in order to the make their own chance of probability success and mainly in this type of method they first try to know your intention if you are not care able about own money their hook you. In order to test your mind using the press of any number or the use of prerecorded call[9].

B. PHONE PHISHING SCAMS

It often seen that every year thousands of people are suffering to phone phishing[9] and due some amount of money lost their life saving money and the scams suddenly increase year to year and in India it also seen that the phone phishing are widely increasing and the scammers use name of higher bank authority profile to make better their chance of success in order tell you about your account or credit has been blocked and I want to reopen them in this entire process they want to take your sensitive information such as private

Information likes your name, address, mobile number, dates of birth and in case of credit card such as card number, cvv number and pin number.

EXPERIMENT

C. PROPOSED PLAN FOR PROTECT AGAINST PHONE PHISHING ATTACK

PHISHING INCIDENT

1. SELF WORK
2. REPORT
3. MOBILE OPERATOR WORK
4. ORGANISATION
5. FINAL

1. SELF WORK

First is the self intelligence power, in this first self control against fraud or phone phishing. Bank or any other financial organization not give you prize even not tell you about claiming your prize and record the phone call when phishers call you.

2. REPORT

In this section you report against phishing to your mobile service provider or other organization such as government or private that work on phishing and special new made organization for the phone phishing.

3. OPERATOR WORK

In this stage basically work for mobile service provider. First operator service provider investigate the reported phone number and give the details of phone number such as name, address, another locality number to newly made organization that work on phone phishing attack and ban it on your service that why it never think the phishing phone again to user.

5. ORGANISATION

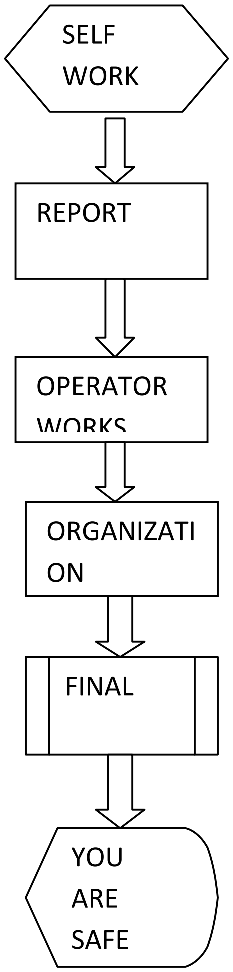
In this section first work for government that first make a organization that work on protect people against phone phishing and work of the organization is the reported phone number such details name, address and reference number arrest them and give them under law order and this section also for Anti phishing organization.

5. FINAL

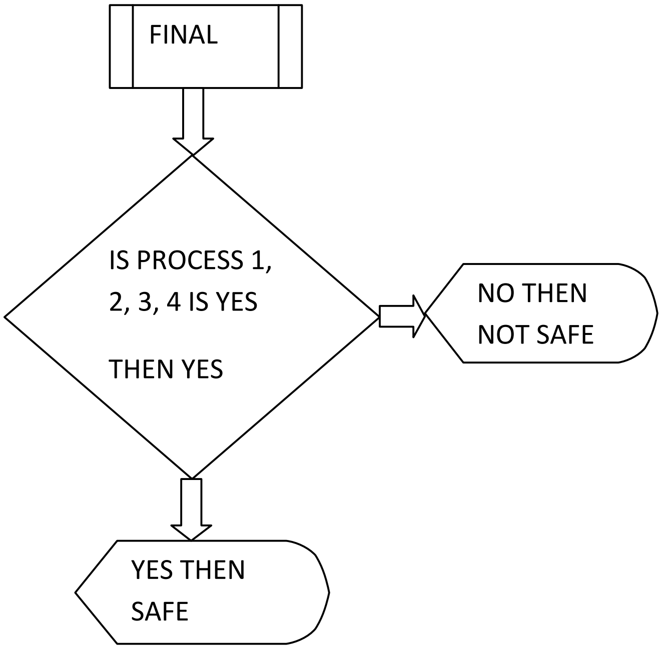
In this stage take care of all the above process, basically send a message to requesting user to report about phishing phone call , check the process two that lies report against phishing phone call coming or not and the process three operator work see operator work or not proper way action taken against phishing phone taken or not. In this section basically work for government authority.

A. FLOW CHART OF PROPOSED PLAN

1.



2.



B. MATH CONCEPT OF PROPOSED PLAN

Here number is shown process number.

Phone Phishing Incident=1+2+3+4+5

Is process 1 is yes then goes to process 2 otherwise no.

Is process 2 is yes then goes to process 3 otherwise no.

Is process 3 is yes then goes to process 4 otherwise no.

Is process 4 is yes then goes to process 5 otherwise no.

Is process 5 is yes then we are safe from the phone phishing attack and if any one of process 1 to 4 are no then process 5 are no that lies all the 1, 2, 3 and 4 process are yes then 5 yes

1+2+3+4+5=Secure against Phone Phishing attack.

C. THEORATICAL PROOF OF PLAN

From the above proposed plan we can see that we are safe from the phone phishing attack. The proposed plan is divided into part of five method first one is the Self work means that self control is main factor in that protect self against phone phishing and in this method you learn about the how to avoid phone phishing target. Now coming to second one Report against phishing if any one target to you for phishing first you report about that your operator service provider such as email service provider or anti phishing organization government or private that working on Anti phishing. After that coming to next one that is Operator works means basically for service provider or Anti phishing organization take strict action about the reported phishing target. And fourth one is the organization in this one first need of organization that work on law and take serious decision against the reported people to the operator in this type of organization anti phishing organization are also come the need of anti phishing organization are also like that in the proposed plan and after that last one is the Final that means how we do all in this method take care of all the above process if any fault in any of the above four process just prepare report about it or send a reminder message to all of above that you do own responsibility that lies tell to user report about phone phishing target that after that phishers not target anyone and technically or operator service provider do own responsibility or not of safe user to the phone phishing attack.

CONCLUSION

From the above result it seen that if we start working now on proposed plan the chance of phone phishing be less and now phone phishing increasing suddenly days to days, from the use of above method the increase phone phishing scams goes down in decreasing order and people are feel safe to the phone phishing attack. Basically from the my thinking one need of government organization that take care of final that I tell in last method and work of organization take care of above three process and time to time send reminder to user , operator service provider and Anti phishing organization to work properly.

Meaning used

Operator service provider- means the in mobile phone sim card provider organization.

ACKNOWLEDGEMENT

First I would like to thanks Wikipedia organization for help in some term and also Aryan jha.

REFERENCES

1. Ramzan, Zulfikar (2010). "Phishing attacks and countermeasures". In Stamp, Mark & Stavroulakis, Peter. Handbook of Information and Communication Security.
2. www.searchsecurity.techtarget.com/definition/phishing.
3. https://en.wikipedia.org/wiki/Phishing.
4. Gaurav Kumar, “Novel Method and Procedure for System Security”, *International Journal of Advance Engineering and Global Technology*, Vol. 3, 2015.
5. Microsoft Corporation. "What is social engineering?"
6. www.antiphishing.org
7. Gaurav Kumar, “Best Plan for System Security”, *International Journal of Advance Research in Computer Science & Technology*, Vol. 3, 2015.
8. Www.Gooogle.Com.
9. http://www.consumer.ftc.gov/articles/0076-phone-scams.
10. https://en.wikipedia.org/wiki/Voice_phishing
11. http://blog.trendmicro.com/trendlabs-security-intelligence/phone-phishing-data-breaches-and-banking-scams/.
12. Gaurav Kumar, “Novel Method to Protect Against Phishing Attack”, *SK International Journal of Multidisciplinary Research Hub*, Vol. 2, 2015.

13. Chakraborty, Shivashish, and Siladitya Sen. "Preventing Desensitization of Radio Frequency Receivers-a Realistic Approach." *Open Journal of Computer Science and Information Technology* 1.1 (2013): 33-38.
14. Gaurav Kumar, "Best Method to Change the Face of Industry Using Artificial Intelligence", *International Journal of Advance Engineering in Computer Science and Management Studies*, Vol. 3, 2015.
15. http://www.bbc.com/news/uk-england-dorset-25986699
16. Baker, Emiley; Wade Baker; John Tedesco (2007). "Organizations Respond to Phishing: Exploring the Public Relations Tackle Box". *Communication Research Reports* 24(4): 327.

AUTHOR DETAILS

GAURAV KUMAR: - He is pursuing the degree in Information Technology from the Maulana Abul Kalam Azad University of Technology (Formerly known as West Bengal University of Technology) Kolkata, India.

Him area of interest are Information Security, Digital Watermarking, Digital Image Processing, Artificial Intelligence, Design and Analysis Of Algorithm, Operating System, Computer Architecture, Cloud Computing, Data structure, JAVA, C, C++, PYTHON.