

A Study on Ethical Phishing on E-mail Networks and its Impacts in India

G. Gopu^{1*} and K. Thangadurai²

¹Dr. GRD College of Science, Avanashi Road, Coimbatore – 641014, Tamil Nadu, India;vggopu@gmail.com

²Government Arts College, Karur - 639 005, Tamil Nadu, India;ktramprasad04@yahoo.com

Abstract

Objective: Phishing is a form of online identity theft that aims to acquire sensitive information from E-mail users such as password. E-mail users faces many security issues while they exchanging information. **Methods/Statistical Analysis:** In this paper we discussed the analysis of psychological and physical conflicts from arrivals of new digital expertise. Due to the desire knowledge of technology and its up-gradations which leads to commit a crime or may aim to target by others. Most of the cyber related crimes committed through E-Mail. To find E-mail phishing various view of analysis were adopted. **Findings:** With this analysis we found the role of phisher in an electronic mail and their way of thinking, planning and executing attacks for their personal gain and as well as for others benefit. **Applications/Improvements:** We improved the accuracy of findings with PHP script and its impacts in India.

Keywords: Countermeasures, E-mail Networks, LAW and Punishments, Survey Finding

1. Introduction

The people in all over the world have ability to communicate with each other by E-Mail, Web log, Cell phone, Texting message and other technological advancements. People do this in hope that they are securing their life by preparing for reduce the level of depression. The communication often leads to the people's real world, physical and psychological conflicts as well as depression, ups and downs.

Moreover, when it is unclear or fake it can lead to misunderstanding in their personal life. The people can become a victim from their movements, due to their desire of using modern technology and their failure to use safe of internet practices or by a computer professional.

2. E-mail Networks

The most commonly referred and preferred mode of communication network is Electronic mail or E-mail. E-mail users have a minimum of one account each and an average of three different accounts per person.

E-mail network is no different from the traditional network, which allow the people to stay in touch with

friends and relatives, share movements of joy and sorrow, transfer important documents, forward meaningless junk to friends, play tricks and even maintain conditional business deals, all within fraction of seconds^{1,2}. More and more people and people in an organization depending upon e-mail for their daily dose of critical communication, some of which may contain personal information, company secrets and sensitive information. Because of it's an importance, crime and criminology activities have been increased such as phishing. Deduction of activities in network is more complicated. Because it involves in different methods and methodologies on E-mail networks such as phishing.

3. Ethical Phishing

Phishing is the form of systematic identity theft that aims to steal sensitive information from users such as user name and password, credit and debit card information's and user's money^{3,4}. A very common example is an email that appears to be individual or organization or E-mail service provider. They might have a message that needs to update your details, or that there is an important security message, and advised to click through a url provided in

* Author for correspondence

the email in order to rectify the situation. When the user clicks through the link, the website might look almost identical to the real website, but there are some hidden differences.

3.1 Who Is Behind the Phishing?

The person behind phishing is human beings, who called phisher. They send out countless e-mails in the hope of few recipient will provide their personal details and financial information for their purpose or for others benefits.

3.2 How does a phishing work?

A phisher uses their knowledge to steal the secured data's on e-mail network using applications such as HTML and PHP⁵. The following information implies that how a phisher might do this, by looking at the steps the password would go through Figure 1.

- Phisher creates replica look of a web page and they save the replica web page of the real website as html file to their own computer⁶. They rename this file to "<filename>. <html>" so that this is the first page that shows up when someone clicks through to the false link.
- Phisher uses their knowledge in script to copy and steal password details when you enter them in replica web page⁷. The following is an example of script phisher uses to steal E-mail user's password from a web page. This would be saved as a PHP file called "<filename>.<txt>"

```
<?php
```

```
Header("Location: https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue=https://mail.google.com/mail/&ss=1&ssc=1&tmpl=default&tmplcache=2&emr=1&osid=1#identifier ");
```

```
$handle = fopen("filename.txt", "p");
Foreach($_GET as $variable => $value)
{
    fwrite($handle, $variable);
    fwrite($handle, "=");
    fwrite($handle, $value);
    fwrite($handle, "\r\n");
}
```

- Next, they incorporate this script into the replica web page, named as "<filename. html>". Then replica web page uploaded to a web hosting service to steal the E-mail user's password.

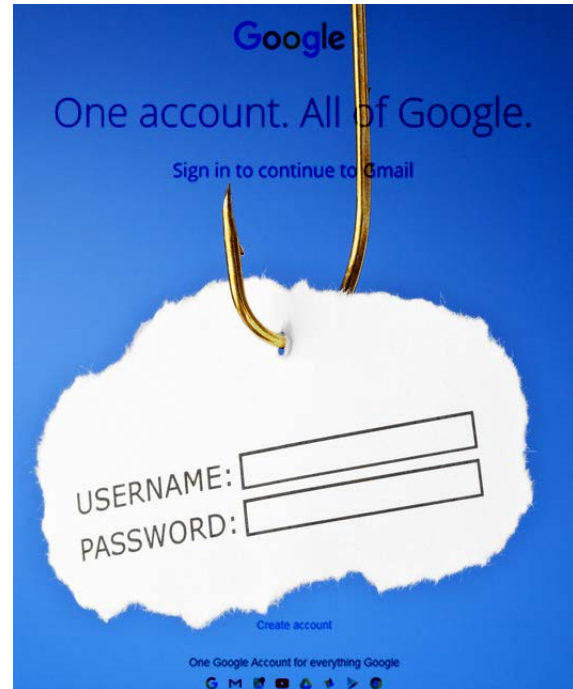


Figure 1. Sample of google login..

4. LAW and Punishments

According to the Information Technology Act 2000, provides legal framework to address various types of crime and prescribes punishment also such crimes.

- Under Section 66 IT Act, describes that "If a person changes by way of deletion of record or alteration of electronic information or data in the account of victim residing in the server."
- Under section 66C IT Act, describes that "If a person disguises himself as an organization such as banker and uses the unique identifying feature of an organization like Name and Goodwill, Logo etc."
- Under Section 66D IT Act, describes that "A person through the use of the electronic mail containing the link to the replica web page of real website to cheat upon the innocent persons."

5. Survey Finding on E-mail Phishing

According to the report from various sources indicated that E-mail related crimes registered in all over the world. These are some of the survey findings in India Figure 2.

1. Income Tax Department has taken necessary steps for safeguarding taxpayers from Phishing email on 5th February, 2016⁸.
2. India ranks at third among countries with high amount of financial Trojan infections, over 60,000 computers in India were compromised with financial Trojans in 2015⁹.
3. May 2014, Delhi Police registered a case in this regard under section 66 of IT Act and section 509 IPC on a complaint filed by TV anchor Amrita Rai alleging hacking of her E-mail account and posting of malicious content on social media with an intention to outrage her modesty¹⁰.
4. India globally fourth place in third quarter 2013 phishing report from RSA. India received 3 percent of attacks during that period¹¹.
5. RBI Warns the public on Phishing Mail on Aug 01, 2014. They said that "Not to give Details of Bank Account or Credit/Debit Cards on Email or over the Phone¹²".

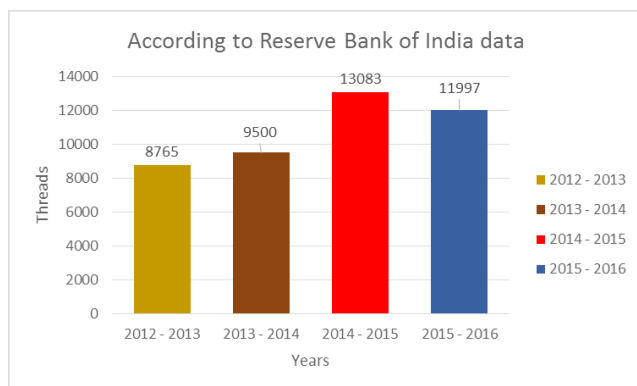


Figure 2. Reserve Bank of India report on phishing attacks..

6. Countermeasures

The people of all the age group including children, teenager, student, parents and business community must keep in mind while interacting with E-mail systems.

- Conducting awareness and training program regarding E-mail and threads is extremely important for E-mail users.
- It is highly recommended to install Antivirus tool to scan all incoming and outgoing E-mails.
- E-mail users are discouraged from giving out their E-mail address to public addresses (like online contests, forums and lucky draws).

- Avoid trust, even E-mails that you receive from your friends or colleagues. Sometimes, infected system with a virus and the malicious code automatically sends copy of itself to everybody in the address box.
- It is recommendable to use a strong password for all E-mail users.
- System and network administrator, email users must disable the "mail relaying" option to prevent E-mail forging attacks on the Internet.

7. Conclusion

A global phenomenon is bound to magnetize many illegal activities through the digital technology. India has taken a key step in regulate digital activities by the implementation and amendment of the Information Technology Act. Giving exclusive powers to the cyber crime police and other authorities to tackle such crimes. Similar efforts have been made by various countries to fight Electronic and digital Crimes. A needed effort is still needed to formulate a law on the use of Internet to control this threatening danger and to achieve a crime free Imaginary Space. Cyber Law targets to prevent crime through the use of penal provisions.

8. References

1. McClure S, Scambray J, Kurtz G. Hacking exposed 6 network security secrets & solutions. 10th Edn, McGraw Hill Publication Company; 2009.
2. Shreeram V, Suban M, Shanthi P, Manjula K. Anti-phishing detection of phishing attacks using Genetic Algorithm. 2010 IEEE International Conference on Communication Control and Computing Technologies (ICCCCT), 2010 Oct 7-9; 2010 Dec 17.
3. Almomani A, Gupta B, Wan TC, Altaher A, Manickam S. Phishing dynamic evolving neural fuzzy framework for on-line detection zero-day phishing email. Indian Journal of Science and Technology. 2013 Jan; 6(1):1-5.
4. Naveen K, Saravanan S, Lavanya M, Vaithayanathan V. Improved CAPTCHA based Authentication for E-mail. Indian Journal of Science and Technology. 2015 Dec; 8(35):1-4.
5. Kumar JD, Srikanth V, Tejeswini L. Email phishing attack mitigation using server side email addon. Indian Journal of Science and Technology. 2016 May; 9(19):1-5.
6. Silnov DS. An analysis of modern approaches to the delivery of unwanted emails (spam). Indian Journal of Science and Technology. 2016 Jan; 9(4):1-4.
7. Ranjith G, Vijayachandra J, Prathusha B, Sagarika P. Design and implementation of a defense system from TCP

- injection attacks. Indian Journal of Science and Technology. 2016 Oct; 9(40):1–6.
8. Reserve Bank of India phishing email[Internet]. [cited 2014 Jan 01]. Available from: https://rbi.org.in/scripts/BS_Press-ReleaseDisplay.aspx?prid=31755.
 9. The Economic Times, phishing report[Internet]. [cited 2013 Aug 22]. Available from: http://articles.economictimes.indiatimes.com/2013-08-22/news/41437405_1_phishing-attacks-rsa-emc.
 10. Government India, Income Tax Department, phishing report[Internet]. [cited 2016 Feb 05]. Available from: <http://www.incometaxindia.gov.in/Lists/Press%20Releases/Attachments/441/Press-Release-Anti-Phishing-email-05-02-2016.pdf>.
 11. Rediff.com, hacking email account[Internet]. [cited 2014 May 02]. 2014. Available from: <http://www.rediff.com/news/report/fir-registered-over-hacking-of-amrita-rais-email-account/20140502.htm>.
 12. India Risk Survey, Phishing activity trends report[Internet]. [cited 2015]. 2015, Available from: <http://ficci.in/Sedocument/20328/India-Risk-Survey-2015.pdf>.