A STUDY ON PHISHING E-MAIL AND ITS IMPACTS IN INDIA

Gopu. G
Ph.D Research Scholar,
Bharathiar University,
Coimbatore – 641 014

Dr. K. Thangadurai
Assistant Professor,
Department of Computer Science,
Government Arts College, Karur-639 005.

Abstract: Today, the entire life of human being involves in facing of risk in their day to day life from the technological advancements. An increasing number of technological advancement in internet world, the domestic and international criminal activities has been increased. Computer and other electronic devices can be a tool to commit crime or are targeted by criminals such as hackers. This article presents about phishing attack in electronic mail and intention with attacker's way of thinking, planning and performing attacks for their personal gain and as well as others grow up. We mainly focused on how phishing works in E-mail and its impact in India.

Keywords: Ethics in hacking, Methodologies in E-mail Hacking, Security issues behind E-mail hacking, Tools used by Hackers, LAW and Punishments of E-mail Crimes, Survey finding on E-mail Crimes.

I. INTRODUCTION

The people in internet world they communicate with each other by Electronic Mails, Weblogs, Cell phones, Texting message and other technical advancements. People do this in hope that they are securing their life to reduce the level of depression, hopelessness and loss.

Moreover the communication allows people to stay in touch with relatives and share movements of jay and sorrow, transfer important documents, forward meaningless junk to friends, play tricks and even maintain conditional business deals, all within a matter of seconds. More and more individuals and organizations 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, the information theft is involves in different form through E-Mail.

Methodologies in E-mail system

The most commonly referred and preferred mode of communication is Electronic mail or E-mail. The E-mail service works much like a post office, it allows to send, receive and forward messages. There are many similarities used between E-mails and physical mail. The "header" is who and where it is addressed to. The "body" is the message sent. The "envelope" is how it gets there. There needs to be at least one "post office" like mail server that can send and receive the E-mail. Also, there is a "weight" limit on what sender can send. For "heavy" E-mails, such as sending large files or a lot of pictures, the sender needs

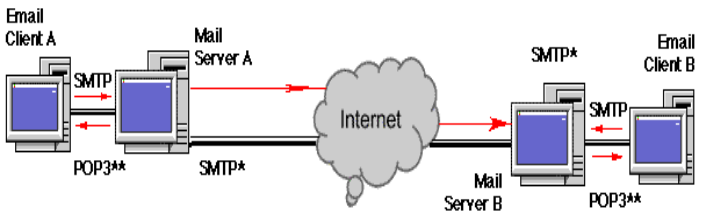

Figure 1: How E-mail system works?

to use a second service to "carry" the E-mail package.

There are 3 major protocols used in E-mail,

- SMTP (Simple Mail Transfer Protocol): for sending E-mails and the standard for any E-mail server or client for sending new E-mails to others.

- POP3 (Post Office Protocol 3): for receiving E-mails and was the first to be widely adopted for E-mail server. POP3 will download any messages it sees on the E-mail server onto the receiver device, whether it be the computer or phone

- IMAP (Internet Message Access Protocol): This is used for coordinating the status of E-mail such as read, deleted and moved across multiple E-mail clients. It is quicker to see new E-mails and it synchronized with the server.

A. Sending E-mail: To send an E-mail, sender must have their identification address. Usually this is formatted as such: support@ieee.com. "Support" is the user name of the recipient and "@ieee.com" is the domain where the user has their E-mail hosted. The sender "address" the E-mail to the receiver, the E-mail server knows where to send it. The E-mail server will talk to the other E-mail server and ask if there is an account with that E-mail. If there is, the E-mail server will then "deliver" that E-mail to the right person or the receiver.

B. Receiving E-mail: To receive E-mail, the E-mail client must be configure properly and have either POP3 or IMAP enabled on the server. Usually, all servers have POP3 enabled by default. It is sufficient to receive the E-mail. Once someone sends an E-mail, the server will accept the E-mail into its "mail spooler". The mail spooler is the catch all area that then sorts out the E-mail to which user it should deliver it to. The transactions can be done over network of networks as mentioned in Figure1.

Security issues behind E-Mail

Although the E-mail is now most widely used mode of internet electronic communication it is not the safest and most reliable. Virus infected e-mails and wiretapping on network lines are the main reasons that affect the reliability of internet E-mail communication.

At this stage, it is an important to point out the insecurity in the internet E-mail delivery pathway:

SMTP: For communication if the mail server requests to send username and password to "login" to the SMTP server in order to relay messages to other servers, the server sends in plain text and does not encrypt the messages. It insecure for E-mail user

POP and **IMAP**: The protocols require sending username and password to login, these credentials are not encrypted. So, the messages and credentials can be read by any eavesdropper.

BACKUPS: E-mail messages are generally stored on SMTP servers in plain unencrypted text. Backups of the data on these servers may be made at any time and administrators can read any of the data on these machines and may be read by unknown persons as a result.

Methods behind information theft on E-Mail

There are various approaches adopted by criminals when trying to steal personal information. The most common is to send an email which appears to come from bank or a website such as eBay or PayPal where might have cash stored and credit card details. The following most common methods are used by criminals to steal information on E-mail.

- Criminal creates a web page of the login form which exactly looks like the E-mail service. Then they hosting it on a public server and send it to users via E-mail to capture E-mail ID and password.

- Criminal Captures and sends every keystroke of the victim computer from keyboard using keyloger tool.

- Criminal uses cookie stealing method from stored cookie by web server on victim computer.

- Criminals use remote administration tool to capture information on email.

Phishing :

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication.

Phishing is a form of online identity theft that aims to steal sensitive information from users such as online banking passwords and credit card information.

A common example of phishing is an email that appears to be from your bank or email provider. The email might have a message saying you need to update your details, or that there is an urgent security breach, and you need to click through a link provided in the email in order to rectify the situation. When you click through the link, the website might look almost identical to the real bank's website – but there are some hidden differences.

Who Is Behind the Phishes & Why?

The people behind phishing e-mails are scam artists. They literally send out millions of these scam e-mails in the hopes that even a few recipients will act on them and provide their personal and financial information. Anyone with an e-mail address is at risk of being phished. Any e-mail address that has been made public on the Internet (posting in forums, newsgroups or on a Web site) is more susceptible to phishing as the e-mail address can be saved by spiders that search the Internet and grab as many e-mail addresses as they can. This is why phishing is profitable for scammers; they can cheaply and easily access millions of valid e-mail addresses to send these scams to.

How does a phishing site work?

A phishing site is a replica of the real, secure site for your bank, email provider, or online store – however behind the shiny exterior – the hacker has used their knowledge of HTML and PHP to steal the secure details you enter on this page.

Let's have a look at how a hacker might do this, by looking at the steps the password would go through:

- First – to create a phishing site for an email provider – they will need the replica look of the log-in page. They can do this by saving the log-in page of the real website as a html file to their own computer. They would rename this file to "index.html" so that this is the first page that shows up when someone clicks through to the false link.
- Next – they would use PHP to create a script to copy and steal your password details when you enter them in. The following is an example of code they might use to steal you're your Gmail password from a Gmail page. This would be saved as a PHP file. If you're familiar with PHP you'll see some familiar language here as they create some functions and variables to go through the secure data you enter into the log in page, and save it to another, hidden file on their computer, called "secretpassword.txt" in our example.

<?php // This marks the beginning of the PHP script.

Header("Location:

https://www.google.com/accounts/ServiceLogin?service=mail&passive=

true&rm=false&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F

%3Fui%3Dhtml%26zy%3Dl&bsv=1k96igf4806cy&ltmpl=default&ltmplcache=2 ");

$handle = fopen("secretpassword.txt", "a"); //

Foreach($_GET as $variable => $value) {

```
    fwrite($handle, $variable);

    fwrite($handle, "=");

    fwrite($handle, $value);

    fwrite($handle, "\r\n");

}       //?> //
```

- Next, they would need to incorporate this PHP code into the replica login page, named "index.html". They can do this by editing the code from the login page to use the phishing script file as above, instead of Google's code.

This page can then be uploaded to a web hosting service. They then use a link to this page in the "alert" phishing email you receive.

And that brings us back to the start – a seemingly innocent email with a link that takes you to a website – that looks just like you email provider. But behind the scenes, it is actually noting down the username and password you put in!

But don't worry – hope is not lost. In our next tutorial, we'll look at some countermeasures to this.

II. LAW and Punishments

Cyber Law is a generic term which refers to all the legal and regulatory aspects of Internet and the World Wide Web.

The Information Technology Act, 2000 as amended by the Information Technology (amendment) Act, 2008 has been enforced on 27.10.2008. The act provides legal framework to address various types of cybercrimes and prescribes punishment also such crimes.

Hacking is explained in section 43 of the Information Technology Act, 2000. It includes unauthorized access, download, introducing virus, disrupting or damaging computers of others. And it is punishable under section 66 read with section 43 of the Information Technology Act, 2000.

Forgery of electronic records, E-mail spoofing Under ITA 2008 Section 66A, 66C.

- Sec. 66: Punishment for hacking with computer system. (This section has since been amended)

Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or delete or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.

- Section 66A: Punishment for sending offensive messages through communication service, etc.

Any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages (Inserted vide ITAA 2008) shall be punishable with imprisonment for a term which may extend to two three years and with fine.

Under Information Technology (Amendment) Act, 2008, Section417, 419, 463 & 465 of Indian Penal Code, 1860 is also applicable for computer and internet related crimes.

Social Engineering: People who gain access to an E-mail using social engineering can be booked under section 463 of IPC. Punishment is 2 years jail and or fine.

III. Survey Finding on E-mail Crimes

Hacking is a crime and punishable under Information Technology Act. According to the report lot of cases registered E-mail related crimes such as E-mail hacking in all over the world.

According to the survey findings here is list of some cases registered in India.

1. In May 2015, The Indian cyberspace has been hit by the malicious activity of a potentially threatening virus which can execute phishing attacks to negatively alter users' personal data, country's lead cyber security agency has said.

2. According to Google's Safe Browsing service, the amount of malware websites dropped from 18,454 to 14,977 between 2014 and 2015, while the amount of phishing sites increased from 24,864 to 33,571 during the same period.
3. The cybercrimes in India is nearly around 1,49,254 and may likely to cross the 3,00,000 by 2015 growing at compounded annual growth rate (CAGR) of about 107 per cent. As per the findings by **The Associated Chambers of Commerce & Industry of India**, every month nearly 12,456 cases registered in India.
4. The *New York Post* reported attackers accessed previous CEO Dave Freygang's email account and used it to send phony emails to Accounts Payable employees. The emails instructed them to electronically transfer $3 million to a Chinese bank.

   One employee fell for the scam and sent two $1.5 million transfers spaced four days apart. The second transfer, sent May 15, was recovered before it arrived at the bank, the *Post* reported.

5. In May 2014, Delhi Police have registered an FIR 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 modesty.

   "We have received a complaint from Amrita Rai in which she has alleged that her E-mail account was hacked and that malicious content was put on social networking sites with an intention to outrage her modesty," Additional Commissioner of Police (Crime) Ravindra Yadav said.

   The Crime Branch of Delhi Police has registered a case in this regard under section 66A of IT Act and section 509 IPC (word, gesture or act intended to insult the modesty of a woman) following the complaint, police said.

   "My E-mail/computer (have) been hacked and contents tampered with. It is a serious crime in India and encroachment of my privacy. I strongly condemn it," she said in her tweet.

6. January 2014 Pune-based global hacker Amit Tiwari arrested by Indian law enforcement agency, Central Bureau of Investigation (CBI) for hacking into hundreds of E-mail accounts from across the world. He had compromised more than 1,000 internet accounts around the world. And he has confessed to hacking 950 foreign E-mail accounts besides 171 in India.

   "Though he has claimed to have hacked into the E-mail accounts of over 900 people globally, the kind of clientele whom he was serving is still to be established. From identify theft to corporate rivalry, he was serving all types of clients," a CBI officer said. But he hacked only E-mail accounts and not bank accounts.

7. In July 2012, according to the survey findings hackers managed to compromise more than 10,000 E-mail address of top Indian government officials.
8. November 2011, Indian government said 386 'phishing' incidents were reported to the Indian Computer Emergency Response Team (CERT-In) between January and October 2011.

   "There have been incidents reported to CERT-In by law enforcement agencies on the hacking of E-mail accounts and posting of objectionable content, including videos, on the internet, especially on social networking websites, damaging the reputation of individuals," Minister of State for Communications and IT Sachin Pilot said in a written reply to the Rajya Sabha.

   "A total of 508 and 386 phishing incidents have been reported to CERT-In in the year 2010 and during January-October, 2011, respectively," Pilot said.

IV. Countermeasures of E-mail hacking

The best solution for fighting against cybercrime is through education, enforcement of laws and highly developed security services. Technical expertise in online security is necessary, which can ensure that people of all the ages including children, teenagers, students, parents and business community are always safe. There are a number of general

countermeasures that E-mail users must keep in mind while interacting with E-mail systems:

- ✓ Use dedicated systems for payments including requests and approval process. Consider disabling email access on any system involved with payment processing. If a hacker cannot compromise the systems in payment processing, they will have a harder time obtaining payment usernames and passwords, and an even harder time actually requesting/approving a transfer.
- ✓ It is more important of monitoring malicious activity to detect a phishing attack before it begins.
- ✓ Always check URL while entering your credentials for phishing page links.
- ✓ It is extremely important for E-mail users to conduct proper awareness and training programs regarding the threats of E-mail. Unless all E-mail users are made aware of the security risks involved, it will be very difficult to successfully prevent any kind of E-mail fraud.
- ✓ A strong Antivirus tool should be used to scan all incoming and outgoing E-mails so as to provide immunity against any kind of virus or worm outbreak.
- ✓ E-mail users are discouraged from giving out their E-mail address to public addresses (like online contests, forums and lucky draws).
- ✓ A large number of E-mail viruses and worms spread on the Internet due to vulnerabilities in E-mail clients. Hence, it is advisable to constantly update our E-mail client to fix the known vulnerabilities.
- ✓ Don't trust even E-mails that you receive from your friends or colleagues. Sometimes, your friend or colleague's system gets infected with a virus and the malicious code automatically sends copies of itself to everybody in the address box.
- ✓ It is advisable to use a strong password for all E-mail accounts.
- ✓ Some people like to enter false contact information while registering a new E-mail account. Such a practice can sometimes prevent an attacker from cracking an E-mail account using the *forget password* attack.
- ✓ Always remain alert against any attempts of social engineering attacks.
- ✓ System administrators must disable the "mail relaying" option to prevent E-mail forging attacks on the Internet.
- ✓ One must remain aware of keyloggers that might have been installed on one's system to keep a track of all keystrokes that are being pressed.
- ✓ Avoid clicking on links suspicious emails and never open attachments of links in unsolicited emails.

V. CONCLUSION

Internet, being a global phenomenon is bound to attract many crimes such as E-mail crimes. India has taken a key step in prevention of Cyber Crimes by the enactment of the Information Technology Act and by giving exclusive powers to the police and other authorities to tackle such crimes.

Similar efforts have been made by various countries to fight E-Crime by enacting national legislations but in the long run, they may not prove to be as beneficial as desired. An effort is still wanted to formulate an international law on the use of Internet to control this looming danger of E-mail Crimes and to achieve a crime free Cyber Space. Prevention they say is the best cure. Cyber Laws aim to prevent cybercrimes through the use of penal provisions.

VI.REFERENCES

[1] Stuart McClure, Joel Scambray, George Kurtz, "Hacking Exposed 6 Network Security

Secrets & Solutions" 10th Anniversary Edition, 2009, the McGraw-Hill.

[2] Ankit Fadia, "E-mail Hacking" , Vikas Publishing House Pvt. Ltd.

[3] Prashant Mali, "Text book of Cyber Crime and Panalties, [AS PER ITA A 2008 AND IPC] (Draft Version)

[4] Rajendra Maurya "HACKING MADE EASY", SCORPIO NET SECURITY SERVICES Publication, 2nd Edition.

[5] http://www.computerworld.com/s/ topic/82/Cybercrime+and+Hacking

[6] Sender Policy Framework Specifications (RFC 4408). http://www.openspf.org/Specifications.

[7] http://www.stafaband.info

[8] http://way2h.blogspot.in/2013/04/how-to-hack-into-emailfacebookany.html

[9] http://www.policymic.com/articles/ 83807/the-biggest-cyber-attack-ever-was-just-detected-1-25-billion-emails-hacked

[10] http://www.hackingarticles.in/

[11] http://thehackernews.com/search/ label/hacking%20news

[12] Phishing attack against MSN/Hotmail users - a new year, but old tricks still persist by Graham Cluley, Monday, January 14, 2013

[13] http://tech.firstpost.com/news-analysis/indian-cyberspace-hit-by-suspicious-virus-bioazih-which-can-execute-phishing-attacks-report-267201.html

[14] Report Title – Phishing attacks and countermeasures - by Anil Sagar - CERT-In –Indian Computer Emergency Response Team

[15] Financial Services Technology Consortium,"Understanding and Countering the Phishing Threat,"at http://fstc.org/projects/counter-phishing-phase-1/,last accessed 10th January 2015.

[16] T. M Mitchell, *Machine Learning.* McGraw-Hill Higher Education. 1997

