ISSN:0975-9646

A Comprehensive Study of Phishing Attacks

Dr. M. Nazreen Banu

Professor, Department of MCA
M.A.M College of Engineering
Tiruchirappalli

S. Munawara Banu

Assistant Professor, Department of IT
Jamal Mohamed College(Autonomous)
Tiruchirappalli

***Abstract*- Now a days one of the highly used techniques to pursue online stealing of data and to do fraudulent transactions is phishing. Phishing is a form of online identity theft that aims to steal sensitive information such as online passwords and credit card information. It is affecting all the major sectors of industry day by day with a lot of misuse of user credentials. To stop phishing many detection and prevention techniques has been made with their own advantages and disadvantages respectively, but phishing has not been eradicated completely yet. In this paper , we have studied phishing and its types in detail and reviewed some of the phishing and anti phishing techniques.**

***Keywords*- Phishing, Anti-phishing, Malware, Web spoofing.**

I. INTRODUCTION

Phishing is a form of online identity theft that aims to steal sensitive information such as online passwords and credit card information[1]. Phishing attacks use a combination of social engineering and technology spoofing techniques to persuade users into giving away sensitive information that the attacker can used to make financial profit. Normally phishers hijack a banks web pages and send emails to the victim in order to trick the victim to visit the malicious site in order to collect the victim bank account information and card number. The information flow is depicted in Fig 1.

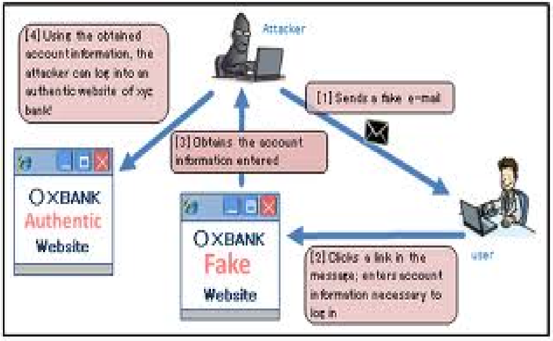

Attacker
[4] Using the obtained accountinformation, the attacker can log into an authenticwebsite of xyz bank!
[1] Sends a fake e-mail
[3] Obtains the account information entered
OXBANK
Authentic
Website
OXBANK
Fake
Website
[2] Clicks a link in the message; enters account information necessary to log in
user

Fig 1: Information Flow in phishing

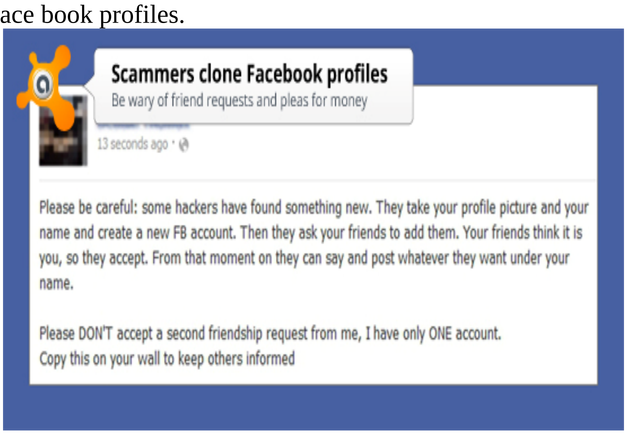
A complete phishing attack involves the roles of phisher. Firstly mailers send out large number of fraudulent e-mails which directs uses to fraudulent websites. Secondly collector set up fraudulent websites which actively prompt users to provide confidential information. Finally cashers use the confidential information to achieve a payout. Goal of this paper is to present on extensive overview of the phishing attacks. The paper is organized as follows. The section II will have an outline of the types of phishing. The section III deals with the theoretical aspects of the phishing techniques. The section IV describes the categories of anti-phishing techniques. Finally conclusion given in section V.

II. TYPES OF PHISHING

Phishing has spread beyond e-mail to include VOIP, SMS, Instant messaging, social networking sites and even multiplayer games. Below are some major categories of phishing.

A. Clone phishing

Clone phishing is a type of phishing attack where hacker tries to clone a web site that is victim usually visits. The clone web site usually asks for login credentials, mimicking the real websites. This will allow the attackers to save these credentials in a text file, database record on his own server, then the attacker redirects his victim to the real websites as a authenticated user[2]. Fig 2 depicts how the hackers clone the face book profiles.


Scammers clone Facebook profiles

Be wary of friend requests and pleas for money

13 seconds ago ·

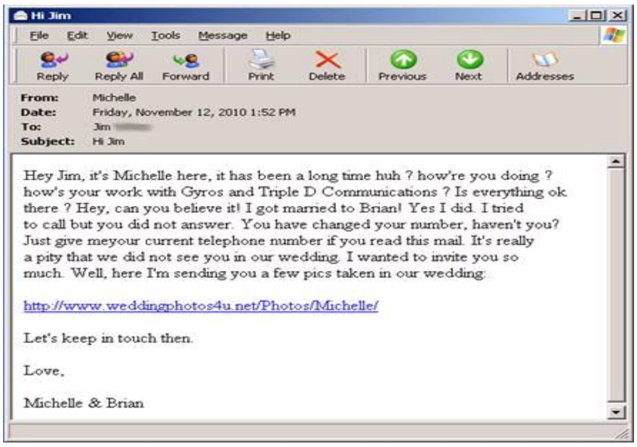
Please be careful: some hackers have found something new. They take your profile picture and your name and create a new FB account. Then they ask your friends to add them. Your friends think it is you, so they accept. From that moment on they can say and post whatever they want under your name.

Please DON'T accept a second friendship request from me, I have only ONE account.
Copy this on your wall to keep others informed

Fig 2: Clone phishing in Facebook profiles

B. Spear phishing

Spear phishing targets at specific group. So instead of casting out thousands of e-mails randomly spear phishers target selected groups of people with something in common[3]. For example, people from same organisation. Spear phishing is represented in Fig 3.


Hi Jim
File Edit View Tools Message Help
Reply Reply All Forward Print Delete Previous Next Addresses

From: Michelle
Date: Friday, November 12, 2010 1:52 PM
To: Jim [redacted]
Subject: Hi Jim

Hey Jim, it's Michelle here, it has been a long time huh ? how're you doing ? how's your work with Gyros and Triple D Communications ? Is everything ok there ? Hey, can you believe it! I got married to Brian! Yes I did. I tried to call but you did not answer. You have changed your number, haven't you? Just give meyour current telephone number if you read this mail. It's really a pity that we did not see you in our wedding. I wanted to invite you so much. Well, here I'm sending you a few pics taken in our wedding:

http://www.weddingphotos4u.net/Photos/Michelle/

Let's keep in touch then.

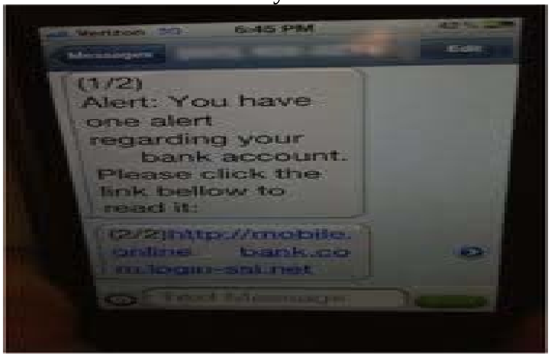
Love,

Michelle & Brian

Fig 3: Spear phishing

C. Phone phishing

This type of phishing refers to messages that claim to be form a bank asking users to dial a phone number regarding problems with that bank accounts. SMS phishing is a variation for phone phishing. The end-users receives sms telling him that he has successfully subscribed to a service[4]. If he wants to unsubscribe the service he should visit the website now the end users visit the websites and provide sensitive information. Fig 4 represents how an attacker gets the user details from the user by SMS.



(1/2) Alert: You have one alert regarding your bank account. Please click the link bellow to read it:

(2/2)http://mobile.online bank.com.login-ssl.net

Fig 4: Phone phishing

D. DNS-Based Phishing (Pharming)

Pharming is an attack aiming to redirect a website traffic to another bogus site. Pharming interfere with the resolution of domain name to an IP address so that domain name of genuine web site is mapped onto IP address of rogue website[6]. DNS based phishing is depicted in Fig 5.

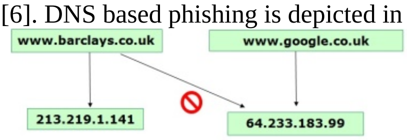


Fig 5: DNS Based phishing

If we are typing the domain name www.barclays.co.uk in the address bar, it is redirected to www.google.co.uk. It is shown in the following Fig 6.

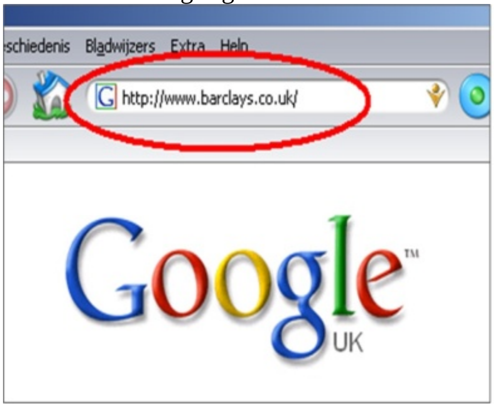


Fig 6: Website redirection

E. Man-in-the-middle-attack

A man-in-the-middle attack often refers to an attack in which an attacker secretly intercepts the electronic messages given between the sender and receiver and then capture, insert and modify message during message transmission[7]. A man-in-the-middle attack uses Trojan horses to intercept personal information. It is shown in Fig 7.

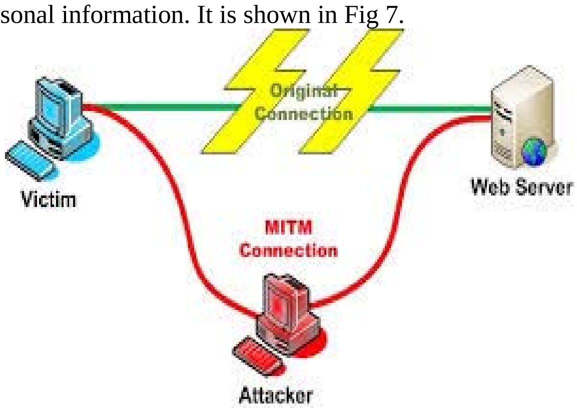


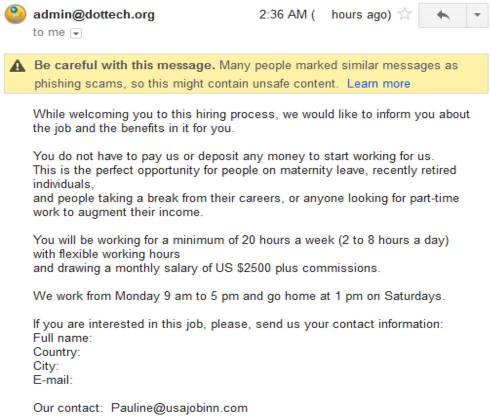
Fig 7: Man-In-The-Middle Attack

III. Theoretical Aspects Of Phishing Techniques

Various techniques are developed to conduct phishing attacks. The phishing techniques are described as follows.

A. Email spoofing

Email spoofing is used to make fraudulent emails appear to be from legitimate senders so that recipients are more likely to believe in the message and take actions according to its instructions. Email spoofing is possible because Simple Mail Transfer Protocol does not include an authentication mechanism. To send spoofed emails sender inserts commands in headers that will alter message information[5]. It is possible to send a message that appears to be from anyone anywhere saying whatever the sender wants it to say. Fig 8 shows the example for e-mail spoofing.



admin@dottech.org 2:36 AM (hours ago)
to me

Be careful with this message. Many people marked similar messages as phishing scams, so this might contain unsafe content. Learn more

While welcoming you to this hiring process, we would like to inform you about the job and the benefits in it for you.

You do not have to pay us or deposit any money to start working for us.
This is the perfect opportunity for people on maternity leave, recently retired individuals,
and people taking a break from their careers, or anyone looking for part-time work to augment their income.

You will be working for a minimum of 20 hours a week (2 to 8 hours a day) with flexible working hours
and drawing a monthly salary of US $2500 plus commissions.

We work from Monday 9 am to 5 pm and go home at 1 pm on Saturdays.

If you are interested in this job, please, send us your contact information:
Full name:
Country:
City:
E-mail:

Our contact: Pauline@usajobinn.com

Fig 8: Email Spoofing

B. Web spoofing

A Phisher could forge a website that looks identical to a legitimate website so that the victims may think this is the genuine site and enter the personal information which is collected by the phisher. Web spoofing creates a shadow copy of the World Wide Web[8]. The shadow copy is funnelled through attackers' machine. Fig 9 shows how does the attacker work.

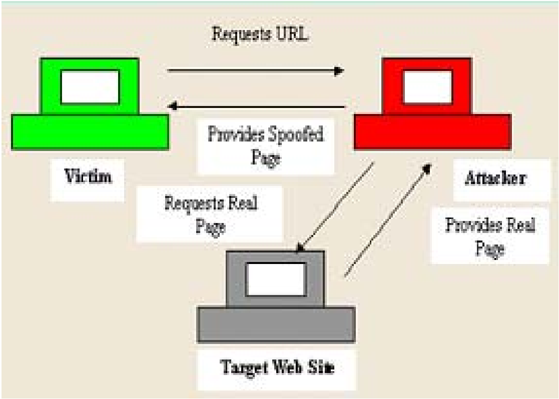


Fig 9: Web spoofing

Modern web browsers have built in security indicators that can including domain name highlighting and HTTPS indicators as shown in Fig 10. They are often neglected by careless users. Modern web browsers display a padlock icon when visting an HTTPS web site of Hyper Text Transfer Protocol and HTTPS, Transport Layer Security, provides encryption and identification through public key infrastructure.

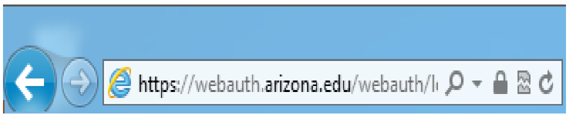


Fig 10: Padlock icon in HTTPS

Web browsers examined the certificate presented by the web browser. The certificate considered as invalid if any of the following situations occurs, the certificate is expired, the certificate is not signed by root CA, the certificate is revoked by CA otherwise the website host name does not match the subject name in the certificate. Fig 11 shows the warning message provided by web browsers. At this moment the browser display a warning and the address bar would turn red.

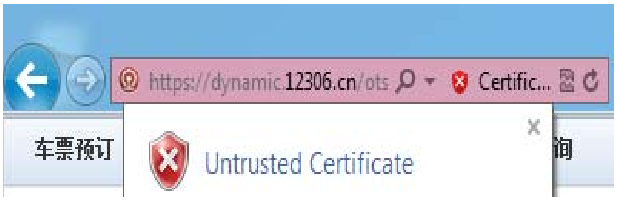


Fig 11: Certificate Verification

C. DNS Cache Poisoning

DNS cache poisoning attempts to feed the cache of local DNS resolves with incorrect records. DNS runs over UDP and easy to spoof the source address of the UDP packet[9]. For example, attacker wants his IP address returned for a DNS query, when the resolver ask NS1.google.com for www.google.com. The attacker could reply first, with its own IP. Fig 12 shows the DNS poisoning attacks.

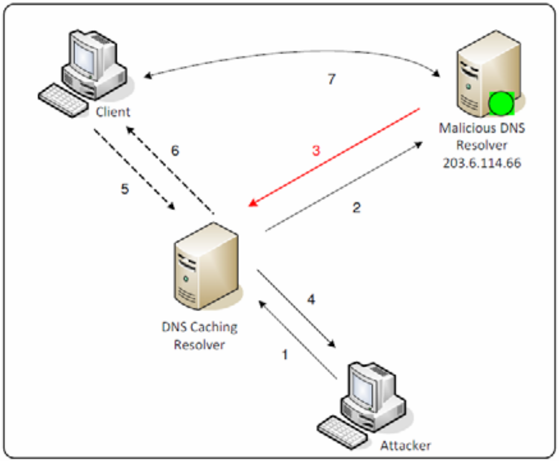
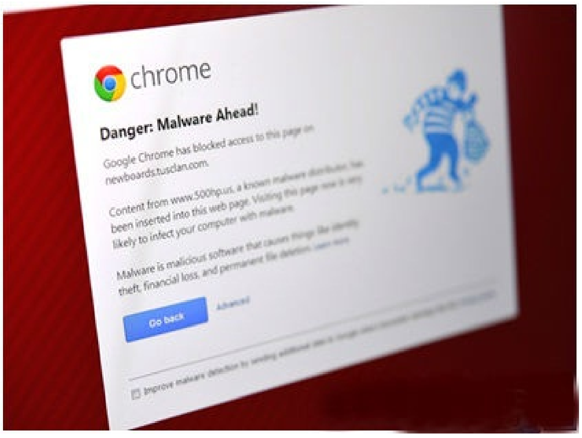


Fig 12: DNS Cache poisoning

D. Malware

Malware is a software used to distrupt computer operation gather sensitive information. It can appear in the form of code, scripts, active content and other software. Malware includes viruses, worms, trojan horses, key loggers, spyware, adware. Client security products are able to detect and remove malware and other potentially unwanted programs. But phishers can make malware undetectable[10]. Key strokes, screen shots, clipboard contents and program activities can be collected and send this information to phishers by e-mail, ftp server or IRC channel. Malware detection is represented in Fig 13.



chrome

Danger: Malware Ahead!

Google Chrome has blocked access to this page on newboards.tusclan.com.

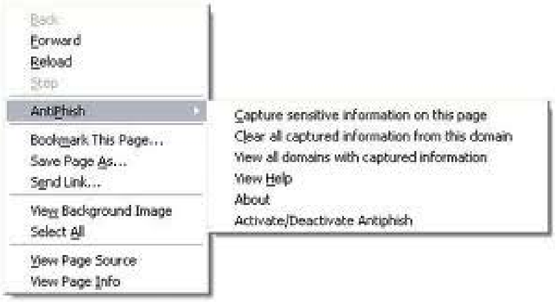
Content from www.500hp.us, a known malware [illegible] has been inserted into this web page. Visiting this page now is [illegible] likely to infect your computer with malware.

Malware is malicious software that causes things like identity theft, financial loss, and permanent file deletion. [illegible]

Fig 13: Malware Warning

IV. Anti-Phishing Techniques

AntiPhish is based on the premise that for inexperienced, technically unsophisticated users, it is better for an application to attempt to check the trustworthiness of a web site on behalf of the user. Unlike a user, an application will not be fooled by obfuscation tricks such as a similar sounding domain name[11]. AntiPhish is an application that is integrated into the web browser that is depicted in Fig 14. It keeps track of a user's sensitive information and prevents this information from being passed to a web site that is not onsidered "trusted".



Back
Forward
Reload
Stop
AntiPhish
Bookmark This Page...
Save Page As...
Send Link...
View Background Image
Select All
View Page Source
View Page Info
Capture sensitive information on this page
Clear all captured information from this domain
View all domains with captured information
View Help
About
Activate/Deactivate Antiphish

Fig 14: Anti-phishing integration in Browser

In general anti-phishing techniques can be classified into following four categories[12].

Content Filtering- In this methodology ontent/email are filtered as it enters in the victim's mail box using machine learning methods, such as Bayesian dditive Regression Trees or Support Vector Machines.

Black Listing- Blacklist is collection of known phishing Web sites/addresses published by trusted entities like google's and Microsoft's black list. It requires both a client & a server component. The client component is implemented as either an email or browser plug-in that interacts with a server component, which in this case is a public Web site that provides a list of known phishing sites.

Symptom-Based Prevention- Symptom-based prevention analyses the content of each Web page the user visits and generates phishing alerts according to the type and number of symptoms detected.

Domain Binding- It is an client's browser based techniques where sensitive information is bind to a particular domains. It warns the user when he visits a domain to which user credential is not bind.

V. Conclusion

Phishing attacks are still successful because of many inexperienced and unsophisticated internet users. The last years have brought a dramatic increase in the number and sophistication of such attacks. This paper provides a broad survey of various phishing types which are used by attackers to steal the sensitive information. This study clearly shows that phishing techniques enables the attackers to steal the information efficiently. Our future work is to compare various types of anti-phishing techniques and choose the best one for further research.

References

[1] Antonio San Martino, Xavier Perramon, "Phishing Secrets: History, Effects, and Countermeasures", International Journal of Network Security, Vol.11, No.3, PP.163–171, Nov. 2010.

[2] Clone Phishing - Phishing from Wikipedia, the free encyclopedia, http://en.wikipedia.org/wiki/Phishing

[3] Bimal Parmar, Faronics, "Protecting against spear-phishing", http://www.faronics.com/assets/CFS_2012-01_Jan.pdf

[4] Phone spoofing From Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Phishing#Phone_phishing

[5] Email spoofing From Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Email_spoofing

[6] John, " DNS-Based Phishing Attack in Public Hotspots"

[7] Mattias Eriksson, "An Example of a Man-in-the-middle Attack Against Server Authenticated SSL-sessions"

[8] Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach, "Web Spoofing: An Internet Con Game"

[9] *Joe Stewart*, "DNS Cache Poisoning – The Next Generation"

[10] Malware from Wikipedia, the free encyclopedia http://en.wikipedia.org/wiki/Malware

[11]Engin kirda, Christopher Kruegel, "Protecting users against Phishing attacks", The Computer Journal Vol. 00, No. 0, 2005

[12] Gaurav, Madhuresh Mishra, Anurag Jain, " Anti-Phishing Techniques: A Review", International Journal of Engineering Research and Applications ISSN: 2248-9622, Vol. 2, Issue 2,Mar-Apr 2012, pp.350-355