International Journal of Students Research in Technology & Management
Vol 3 (01), January 2015, ISSN 2321-2543, pg 216-222

Phishing: An Evolving Threat

Phishing and forms combined with Social Engineering

Keyur Shah, Tanushree Shenvi, Karan Desai, Reshad Asrani, and Varun Jain

Mukesh Patel School of Technology Management and Engineering Mumbai, India

***Abstract* — Phishing is one of the most common attacks used to extract sensitive information for malicious use. It is one of the easiest ways to extract confidential data on a large-scale. A fraudulent website/e-mail which looks very similar to the original is setup to trap the victim to give away confidential information. A large population of internet users still lacks knowledge to avoid phishing. When the phishing attacks are complimented with social engineering skills, the success rate is increased. Along with the progress of technology, phishing techniques have evolved encroaching upon newer communication mediums like voice and text messages giving rise to newer specialized forms of Phishing called - Vishing and SMSishing. In this paper, we also cover how to avoid being a victim of these attacks. One of the best promising methods to avoid Phishing is Zero Knowledge Authentication - ZeKo which immunes the user from phishing attacks.**

***Keywords*—Phishing, Vishing, SMSishing, Social Engineering, ZeKo**

I. What is Phishing?

Phishing is type of internet fraud that uses false or deceptive content to trick users and extract information from them. Phishing historically used e-mails as a medium to reach its target, but soon spread to other forms of communication like websites, SMS's (SMShing), VoIP (Vishing), etc.

From Its initiation in the early 1990's phishing has become one of the most severe threats to computer security systems in modern times. Phishing uses social engineering techniques to engage user on forged site or conversation and then obtain information from him. Phishing is generally used to extract usernames and passwords. Since its main exploit is the user awareness of the working of the web, it is often carried out it bulk or on a large scale to be effective or gain considerable benefit. However, some forms of phishing maybe target to a certain organisations and not everyone. Such types of phishing attacks are categorized as "spear-phishing".

Information once obtained can then be used for identity theft on internet and gain access to valuable accounts like that of banks and other institutes for monetary and other benefits.

II. Some Statistics

In 2003, David Jevans founded the Anti-Phishing Working Group which is an international consortium for all the businesses, government agencies, law enforcement agencies, security products and services companies, communications companies affected by phishing attacks. It has currently more than 3200 members from more than 1700 companies and institutes which include leading security companies like McAfee, BitDefender, VeriSign, Symantec, IronKey and Internet Identity.

Phishing has over the years increased with the growth of web commerce, currently attaining epidemic proportions. Symantec's reporting system recorded about 1,088 phishing e-mails on a daily basis for the in first six months of 2007 which was an 18% increase as compared to last six months of 2006.

In the year of 2006, the rate of response to the phishing e-mails were estimated to be 19%, 5% of which revealed critical information. Among those 45% reported that the information was used to perform monetary transactions In 2007 a study estimated that at 0.4% of users had revealed their usernames and passwords to attackers. The financial services industry has suffered a loss due to the phishing epidemic.

III. The Reason why Phishing Prevails?

A. Lack of Knowledge

1. Lack of computer system knowledge:

Most users do not know how things like email, World Wide Web (WWW), applications and the operating systems work and the difference between these. There are many ways how phishing sites would exploit this. For example, they may exploit user's lack of know-how of a basic URL format which makes it unable to differentiate between a legitimate or a forged site (e.g., they may think www.facebook-user-security.com belongs to www.facebook.com). Another exploit is to modify the email header; many users cannot distinguish forged from legitimate headers.

2. Lack of knowledge of security indicators:

Security indicators are not understood by many people. Most users do not know that the closed padlock icon which appears in the browser denotes that the page currently being displayed was transmitted securely by using SSL. Even if they do know the meaning, they can still be fooled by the icon appearing in the body of the page. The fact that different browsers show the icon at different location adds to

this confusion. Some people do not realize that the padlock icon appears only under specific conditions when SSL is used. Icons can be arbitrarily added by the designer to the page to induce trust.

3. Lack of understanding of the verification process:

Many users do not know where to check the SSL certificates in the browser and they do not understand their contents. In one of the spoofing strategies, a forged site shows a certificate authority (CA)'s trust seal which links to a CA's website. This website provides a simple description and verification of the legitimate site's certificate. Only the most careful users would check the URL of the original site and the legitimate site URL described by the CA match.

B. Visual Deception

1. Visually Deceptive Text:

In "typejacking" attacks the change the domain name slightly by using a similar looking letter , in place of original , such a substitution might go unnoticed (e.g. www.goog1e.com substitutes the number "1" in place of the similar looking alphabet "l"). Non-ASCII and non-printing Unicode characters can also be used in domain names.

2. Images masking underlying text:

A common technique for phishing is to use an image of links of original websites. The image itself serves as a link to a fraud site.

3. Windows masking underlying windows:

One of the most common phishing techniques is to place a fraudulent window besides a legitimate window. If the design is similar and overall theme is same, users mostly consider them from the same source, inspite of variations in domain or other security indicators. In the case of borderless browsers, users may not even notice the distinction between two windows.

4. Deceptive Look and Feel:

If legitimacy signs like logos and design are copied successfully, the only point of distinction a user might have is that of unprofessional design and changed tone. If the forged is made to closely resemble the original site, the only point of distinction might be the request of additional user information from the user.

C. Bounded Attention

1. Lack of attention to security indicators:

When users are performing their primary tasks on the site, security becomes a secondary issue; they generally do not pay attention to security warnings and indicators. The image-hyperlink technique mentioned above would be caught if the user notices the image URL and URL of the image, but that requires very close inspection. Users who know the meaning of a padlock icon, simply observe it without observing its location, i.e. whether it is inside or outside the webpage.

2. Lack of attention to the absence of security indicators:

Absence of security indicators is not noticeably realized by the users. When there are no indicators it becomes possible to enter a spoofed image as indicators.

IV. Study on User's Response to Various Kinds of Phishing Techniques

A. Distinguishing Legitimate Websites

Participants were presented with websites that seems like they belong to e-commerce companies and financial institutions, some real and some spoofed. The participants were given a task to identify fraudulent and legitimate sites and explain the reasoning for the decisions they take.

B. Collection and Selection of Phishing Websites

A web archiving application was used to collect about 200 unique phishing websites, which included all links, images and pages upto three levels deep of the site. To go to these sites, they were provided with a phishing e-mail.

C. Study Design

Every participant was made to see every website, sequenced randomly. Everyone was seated in a university classroom. An Apple G4 Powerbook laptop which was running MAC OS X was used with the Mozilla Firefox browser.

Participants were presented with 20 websites; of which first 19 were in random order:

- 9 representative phishing websites
- 7 legitimate websites
- 3 advanced phishing websites
- 1 requiring the users to agree to sign to a self-signed SSL certificate

D. Scenario and Procedure

The participants were provided with a scenario that they have received an email which asks them ti click on the link of either a fraudulent or legitimate sites. They can interact with the websites as normally users would. Multiple copied of the websites maybe present and they could fraudulent or legitimate irrespective if the website had appeared before.

E. Results

Type 1: Security indicators in website content only

23% of the participants used only the contents of the displayed webpage to determine if the webpage is legitimacy; this included layout, logos and graphic design, absence of presence of functioning images and links, language, type and accuracy of information presented.

Type 2: Content and domain name only

36% of the participants used the URL present in the address bar to make decisions along with the content factors that are mentioned above.

Type 3: Content and address, plus HTTPS

9% of the participants depended on the factors mentioned above but also checked the presence of "HTTPS" in the address bar.

Type 4: All of the above, plus padlock icon

23% of the participants depended on all of the factors mentioned above and also looked for a padlock icon in the browser.

Type 5: All of above, plus certificates

9% participants depended on all of the factors mentioned above and also checked the certificate that was presented to their browser in our study.

V. ZEKO

In order to overcome the majority of the vulnerabilities exposed by phishing, the Zeko authentication procedure was proposed.

The following process describes ZeKo authentication:

A. Setup Procedure

The setup procedure is used to initialize the authentication data at both the server and the client for future authentications. The client acquires two separate authentication elements, namely a token and a password. The server obtains its own authentication element that can be used to authenticate itself and check the responses from the client. A secure channel should be established in order to do the setup for the authentication.

1. The client and the server establish a secure channel using Transport Layer Security to perform the initial setup process. This secure channel will be used to communicate data over rest of the session.
2. The server generates a large random number and sends it to the user as a token. The server deletes the taken from its memory as soon as the client receives the token, since it is no longer needed there. It is recommended to erase the token, since in the case that the server is compromised, authentication elements are not revealed.
3. As soon as the client receives the token from the server, it decides upon a password. The password need not be unique or complex in order to be secured, but it should also not be trivial. With the password and the token as the input, a strong one-way hash function is used to calculate hash value, and the client then uses this hash value for creating a pair of asymmetric keys, P and p-l. Any content that is encrypted using P can only be decrypted using P-l, and vice-versa. P shall be used for client authentication while p-1 will be sent to the server using a secure channel. The user can cache both the keys for faster future authentication, but that will pose a security risk. The user can instead keep the token and the password and generate keys as and when required. The server receives the p-1 and username and stores this information for future authentication.

B. Authentication Procedure

Phase 1: Authentication of server to client

1. The client creates a unique number for this session called nuance. It then encrypts that and its IP address using P (the asymmetric key from setup process). A random number and a timestamp is included to make the transmission unique. This encrypted information is sent to server along with username and password. Inclusion of IP address prevents relay and man in the middle attacks. While the man in the middle attacks could reuse an old authorization or act as a pass way for a legitimate user, the IP address included in the packet will not match. The server obtains the IP address of the client by decrypting it using p-1 obtained during setup procedure. The server checks the IP address of the client as a test, if not matched, a really attack is assumed to have happened.
2. The server then uses its own decryption key p-1 and r1 as inputs to a strong hash function. The server generates another unique number r2; it then transmits the number and the generated hash to the client. On reception the client gets the hash of r1 and p-1 as well as r2, it confirms the hash by calculating it again using p and r1. A match in the hash means that the server it is communicating with is using p-1 and has successfully decrypted r2 which is thus a successful authentication.

This ends server authentication.

Phase 2: Authentication of client to server

It consists of two steps below:

1. After validating server in phase 1, the client then hashes both the random numbers generated by either entities, encrypts the hash with the key P, and sends this encrypted text to server.
2. The server then generates the same hash, using the same numbers as used by the client and matches it with the data that is received from the client. If the data matches it means that the client was successful in decrypting r2 and hence it is the one that uses P and is hence authenticated.

VI. SOCIAL ENGINEERING

Social Engineering is an art or specifically a skill to manage people or human beings to make them do different actions or used to take out confidential information. Social engineering focuses on how our personal or professional relationship can be used to take out the required information from a particular individual.

It becomes very easy to break into a company's or an individual's confidential information if we know that particular person or any employee in that company. Social Engineering basically means using social relationships to get confidential information.

The most important step in Social Engineering is to establish trust with the target. The target here is that individual who is used to extract confidential information. To establish trust even a small talk could be enough provided he is an alert social engineer. The social engineer needs to know the basics, which is to understand whether the target is hesitant and be alert to manipulate the conversation to get the target into confidence. Once the social engineer establishes trust and gets the target in confidence, it is relatively very easy for him to get started with the attack. Once the trust and confidence is established, the target might just give confidential information like a phone number or maybe some password to the social engineer on his request. The social engineer might target different employees of the same company to carry out his attack and get different information from different targets. A social engineer shall avoid asking suspicious questions that shows his motive to avoid making the target hesitant. When the organization is larger, it is easier to gain trust whereas when the organization is smaller, it is more difficult. In a smaller organization, they can be easily identified but in a bigger organization, not all employees would know all other employees. Hence, it is easier to establish trust in a bigger organization.

If the attacker has an information or knowledge of how the internal system of how the organization works, it becomes easier for him to crack into the system and extract confidential information. By this the other employees could just easily trust the attacker considering him as one amongst them.

Another method is reverse engineering to gain trust. In reverse engineering, the three steps are: Sabotage, Advertising and Assisting. In reverse engineering, a scene is created in which the attacker would first help or perform a favor to the target. In return of the favor, the target shall give out confidential information easily as he would trust the attacker.

Clout is another way to get confidential information from the target. Here, the attacker poses as an authoritative person for example, a manager and demand the required information. The attacker can also pose as someone talking on behalf of the management.

Using technology in compliment with the social engineering attack can increase the chances of getting the required confidential information. For example, if there is a spoofed mail from someone in the management (like a CEO) asking to change their passwords to "xyzabc1" or maybe a login system with a Phisher, there is an increased chance of getting sensitive information.

Getting into the workplace physically makes the social engineering attack a lot simpler. The attacker might just follow an employee or take a job with the maintenance/cleaners contractor to gain access into the building or the workplace.

VII. VISHING

Vishing could be termed as a kind of phishing which uses the telephone system to get the required confidential information. It is a Social Engineering technique for stealing information from the target. Vishing is a combination of words – Voice and Phishing. The Vishing attack is generally facilitated by Voice over IP (VoIP). Instead of being directed to a phishing website, the user is asked to make a phone call. The phone can then trigger a VRS (Voice Response System) that could then ask for confidential information like credit card number or the CVV number.

As the target is entering the confidential or sensitive information over the phone, Vishing could be very effective. VoIP is used because it becomes tougher to trace the attacker as the caller IDs can be spoofed and an entire attack setup can be there for a very short period of time.

A popular way to carry out Vishing attack is Wardialing. It uses an automated system to identify the numbers which could be used to call the target according to his area. This makes the call seem legitimate and hence the target falls into the trap. Once the target answers the phone, he could be then asked to give away the sensitive information and the call is recorded.

Another method used to carry out Vishing is Mailbox Raiding and Dumpster Diving. The mailbox of the target could provide more personal information which could be then used to get the user in confidence. The attacker can also get a list of client phone numbers from an organization like a bank, he can feed the numbers into a system and a more systematic and legitimate attack could be carried out.

VIII. SMSISHING

SMSishing is another way to get the required information from the target. SMSishing is an amalgamation of the words SMS and Phishing. Here we use the short messaging service to carry out the phishing attack. In this type of attack, the attacker takes advantage of the target's fear of losing or excitation of gaining.

The SMS which are used to carry out the attack could be something like – "Dear Shoppers Stop customer, Congratulations you have just won a Rs. 10,000 Gift Card." When the target tries to claim the prize by either calling (vishing) or visiting the fraudulent website (phishing), the confidential information can be then easily retrieved. It's a basic human mind set to be excited on seeing messages like these and give away sensitive information when asked for.

Another message could be something like – "Please review your bank account information to avoid blocking of your account" or "Your ATM card has been suspended. To re-activate, call at this number". Here, the target would have fear of losing his account. In this matter, he would readily give out all the sensitive information to the attacker as it seems it would help him save his account.

However, to carry out SMSishing in an effective manner, the attacker must have good social engineering skills. Also, after repeated news broadcasts and awareness programs the success rate of SMSishing has gone down.

IX. How Social Engineering helps in SMSishing and Vishing

Social Engineering is an important aspect while performing a Phishing attack. The phishing attack can be carried out with more ease if the attacker has polished social engineering skills. After the different awareness programs, the population falling for Phishing attacks have gone down to something as low as 9% (as mentioned earlier). However, if the phishing attacks are complimented with a proper social engineering skill, there are better chances of getting the required information.
This can be proved with the help of a few scenarios:

Scenario 1: Using Clout

When a spoofed e-mail comes from the higher management linking to a Phisher, there is a higher probability that the employees would fall into the trap rather than when someone emails randomly.

Scenario 2: Using communication skills

Impressive communication skills and knowing internal jargons could always help to get confidential information. The attacker could call the reception asking to give out confidential information. However, if the social engineering skills are not used, this is impossible. The receptionist would always be hesitant on giving out confidential information.

Scenario 3: Exploiting Trust

In general, in a group of friends in an organization, if one gives them link to the fraudulent or phishing website, there are more chances for them to fall in the trap rather than a stranger trying.

Scenario 4: Physical Access

If the attacker gets access to the workplace physically, he could directly use someone else's account to send the fraudulent mail. If at all the access is to the management's computer or e-mail he could make Phishing very effective.

These scenarios prove that Phishing or Vishing in compliment with social engineering is more effective rather than phishing alone. Developing social engineering skills shall always be helpful while doing a Phishing or a Vishing attack.

X. Defending Against Social Engineering Attacks

In this next session we shall discuss about how to defend from Social Engineering attacks. A good social engineering defense attack would include the following: Data Classification, Password Policies, Termination Process, Security Awareness Training, Acceptable Use Policy, Incident Response, Vulnerability Assessment, Background Checks and Physical Security.

Data can be classified as: Top Secret (highly sensitive material), Highly Confidential (data that can negatively affect the organization's operation if made public), Proprietary (Information of a proprietary nature), Internal use only (information that cannot be circulated outside the organization), Public Documents (information in the public domain).

A good password policy should ensure that the employees cannot write down their password, periodic password change, password standards(alpha-numeric, special characters), methods for password delivery, not sharing passwords, not using default passwords, not writing down passwords, methods for identifying users for password resets and login failure lockout (after three wrong attempts, the account should be locked).

When an employee leaves the company, all the accounts shall be closed and the permissions to access information and physically entering the workplace shall be revoked. Even when an employee is on a short leave, the account should be locked or terminated.

A proper and timely security awareness program should be made compulsory for all the employees. In the security awareness program, it should be explained how to identify an attacker/social engineer and how to react to it.

An acceptable use policy should be enforced to tell employees how the information system should be used. It should cover points like unacceptable e-mail usage, attempting to gain access to unauthorized resources, abuse of internet connectivity, forgery/misrepresentation, commercial use of information/resources and providing authentication credentials to unauthorized users should be prohibited.

A proper background check of the employee should be made before he enters the organization. The attacker might enter the organization and then carry out the attack and hence a proper background check is very important.

Physical Security is another aspect while defending against social engineering attacks. A track of each and every

person entering or leaving the organization - be it a visitor or a courier delivery guy should be kept to ensure physical security. Temporary badges could be issued to the visitor or non-employees.

A. Protection from Phishing

- The most important is being aware and alert. Being alert would help in identifying phishing websites.
- Check the URL of the website. If the URL of the website doesn't matches exactly to the original legitimate website, no sensitive information should be given. Instead of using the link provided in the e-mail, the link should be opened by typing in the official link in the address bar. No links from unknown source or organization should be opened. Advance phishers might also steal cookies and saved passwords just when the link is clicked on.
- Should look for the padlock sign i.e. that signifies a secure connection.
- Should look for the sign of suspected web forgery. It is generally present on the address bar, and if it is present, the website is fraudulent.
- The source of all e-mails that ask for sensitive information should be verified. This can be done by checking e-mail headers that would return the original IP address. The website's HTML should also be checked. This is known as Heuristic based phishing detection.
- Use of password managers can also help to avoid phishing. The password managers could use identification procedures to detect phishing websites which the human eye might miss.
- Use of Internet Security programs can also be of use as they have phishing protection as well.

B. Protection from Vishing

- The best way to avoid falling into a trap is to be educated. All the banking websites provide notices and information and alerts on vishing. When the user is alert, better are the chances to not fall in trap.
- When a person claims to be an authoritative person or on behalf of some particular organization, we should not plainly believe it. Instead, once the phone is disconnected, to verify, the legitimate numbers from the organization's website should be called and asked if such information was demanded for. If a fraud is attempted, the organization or the concerned individual should be reported.
- Also, when a person asks for sensitive information, we should ask questions to verify their identity.
- The phone should be registered for NDNC (National Do Not Call) at http://donotcall.gov.
- All calls like these should be documented or recorded and reported to avoid any future problems.
- Sensitive information like password, bank account number, credit card number or CVV number should never be given over telephone.

C. Protection from SMSishing

- Be aware from the messages that come from the number "5000". Here, the actual number is not shown and it usually indicates that some e-mail or software was used to send the message.
- Never reply to a text that looks suspicious without verifying the identity of the sender.
- The bank's policy on sending messages should be reviewed. Here all legitimate numbers/short codes shall be given by the bank.
- The feature of blocking text messages from internet shall be enabled if available.
- All messages that show some immediate gain without any efforts is generally fake. One should not fall into traps like these.

CONCLUSION

In this paper we have studied one of the most prominent security threats in our society today. Phishing exploits the user's lack of awareness and knowledge towards the various security indicators at his disposal. It deceives the user's by using fraudulent content taking advantage of his inability to distinguish between authentic and forged information. We have analyzed a study which notes the response of average people on recognition of legitimate sites. Current security measures depend on attributes like human awareness and knowledge in order to detect and prevent phishing which is proven to be inadequate over time. To overcome this, we have looked into a promising approach which uses the concept of Zero Knowledge authentication and its functioning. By studying the social aspects of human behaviour towards phishing as a part of human engineering, it is clearly visible that the attackers can easily take advantage of naive users by befriending or threatening them to extract confidential information. In modern times, new technologies like VoIP can be used to bypass generally accepted authentication methods like caller ids. Popular mediums like text messages have been targeted by phishing communities to develop a new form of phishing - SMShing.

Thus it is easy to see, that ever since its initiation phishing has continued to remain a dominant security threat consistently evolving with the latest technologies. The success of these attacks is credited to its persistent fixation on absent minded nature of the users. We believe that advanced authentication techniques like ZeKo could be used as a powerful counter-measure leading us into a better and more secure tomorrow.

REFERENCES

[1] Paul Knickerbocker, Combating Phishing through Zero-Knowledge Authentication, Department of Computer and Information Science and the Graduate School of the University of Oregon

[2] A Karakasiliotis, Assessing end-user awareness of social engineering and phishing, 7th Australian Information Warfare and Security Conference.

[3] Aaron Dolan, Social Engineering, SANS Institute InfoSec Reading Room.

[4] John Aycock, A Design for an anti-spear-phishing system, Virus Bulletin Conference 2007.

[5] Rachna Dhamija, JD Tygar and Marti Hearst, Why Phishing Works, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.