International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 4, April - 2013

# Anti-Phishing Framework Based On Stego-Cryptic Images: A Survey

Mr. Harshal S. Kale
*JSPM's RSCOE,*
*Tathawade, Pune*

Mr. Akash A. Manuja
*JSPM's RSCOE,*
*Tathawade, Pune*

## Abstract

*Phishing is an attack which is used by an attacker i.e. hacker, to illegally acquire and use/misuse someone else's i.e. normal (legitimate) user's important data for the attacker's benefit (e.g. stealing of credit card details during online transaction) . Now-a-days it is affecting the major sectors of industries and misusing the legitimate user credentials. Various anti-phishing techniques have been proposed and implemented to protect the user against phishing attacks. They usually follow different strategies like client side and server side protection. This paper gives a detailed survey of phishing (which includes attack process and classification of phishing attack). It also reviews some of the existing anti-phishing techniques including their advantages and disadvantages.*



## 1. Introduction

### 1.1. Phishing

The primary target of a phishing attack is to illegally carry out financial frauds. This is done by forging an e-mail which leads to a fake website used to masquerade as a legitimate or an official website (e.g. a bank website or a government website). The attacker or the hacker who uses the technique of phishing is usually referred to as a phisher. A phisher is an expert at the art of enticing or luring a user (a victim) in giving up his/her important credentials like Social Security Number, PAN number, Credit/Debit card numbers.

The attacker sends a forged e-mail containing a link to the replica of the original website, as bait, to the user. If the user falls prey to this i.e. he/she gives up the credentials, the attacker saves this data for any sort of misuse.

### 1.2. Cryptography

Data that can be read and understood without any special measures is called *plaintext* or *cleartext*. The method of disguising plaintext in such a way as to hide its substance is called *encryption*. Encrypting plaintext results in unreadable gibberish called *ciphertext*. You use encryption to ensure that information is hidden from anyone for whom it is not intended, even those who can see the encrypted data. The process of reverting ciphertext to its original plaintext is called *decryption*.

### 1.3. Steganography

Steganography is a technique that allows concealed transfer of information over an unconcealed connection. Combination of stealthy channel exploits and the cryptographic technique of substitution ciphers and/or one time pad cryptography, steganography enables the transmission of information embedded inside a file plainly. The hidden data is both difficult to detect and when combined with known encryption algorithms, equally difficult to decipher.

## 2. Literature Survey

Phishing attacks targeting consumers remained at high levels during the quarter. There are hundreds of phishing websites established online every day, and each campaign can involve hundreds of thousands or millions of e-mails sent to consumers. During the third quarter, we saw a constant decline of unique phishing sites detected by the APWG, a trend continued from the second quarter. September 2012's 46,895 sites were slightly below September 2011's 48,410 sites, marking a return to historical phishing levels after a period of high activity. The drop from April to September was 26 percent [1].

**Fig 1: Phishing activity trend report [1]**

Financial services continued to be the most targeted industry sector in the third quarter of 2012. Attacks against financial services and payment services remained steady from the second quarter. Attacks against auctions sites rose from 2.3 percent to 4.5 percent, and attacks against government sites fell slightly.

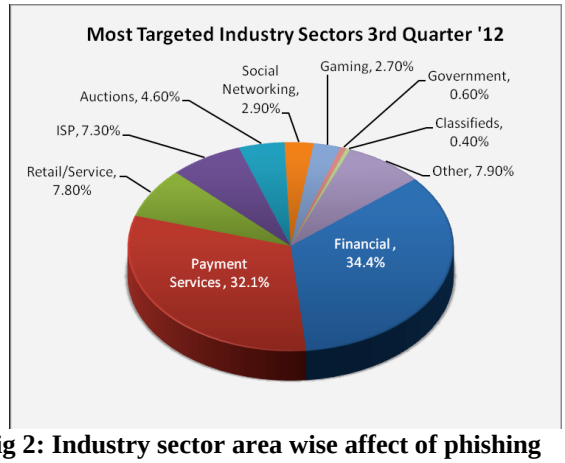


**Fig 2: Industry sector area wise affect of phishing [1]**

## 2.1. Types of phishing attacks

**2.1.1. Deceptive Phishing.** This is the most common type of a phishing attack. It is usually carried out using a fake e-mail which demands the user to verify his/her account by entering the account details. The attacker then records these details for further misuse.

**2.1.2. Malware-Based Phishing.** This type of phishing attack usually requires a malicious application to be downloaded on the victim's computer. The attacker does this by attaching the malicious application (malware) to an e-mail and sending it to the victim.

**2.1.3. Web Trojans.** These are the pop-up windows that pop up invisibly in an attempt to record the user credentials while the user tries to log in. It then sends the recorded information to the attacker.

**2.1.4. Host File Poisoning.** A lot of small and medium business organizations (SMBs) do not have the DNS (Domain Name Systems) to resolve the URL to IP address translation. So, the computers resolve these issues by consulting with the "Host" file in the OS. If an attacker manages to poison this file i.e. re-route the user to a fake website, the user credentials can be stolen easily.

**2.1.5. System Reconfiguration Attacks.** An attacker can modify the settings on a user's PC for malicious purposes. For example, the site tagged as favorite site in a user's PC, "www.gmail.com" can be reconfigured as "www.gmai1.com".

**2.1.6. Pharming (DNS-based phishing).** The optimal target for an attacker here is the DNS of any company. During the address resolution phase, the DNS can be poisoned to return any fake address which may lead to a phishing website.

**2.1.7. Content Injection Phishing.** This is an advanced attack. The attacker attempts to inject or insert a piece of code on a legitimate site to fool the user into giving his/her credentials.

**2.1.8. Man-in-the-middle Phishing.** It is very hard to detect this kind of phishing attack. The attacker acts as a sniffer (man-in-the-middle) who just watches and records the transactions carried out between a customer and a merchant. The attacker does not interrupt or disrupt anything in between the transactions. This makes it hard to detect the attacker. The information he records contains the financial details about the victim (customer) which the attacker can misuse later.

**2.1.9. Search Engine Phishing.** The scammers are very popular to be known to use this type of phishing attack. They set up false advertisements and links offering the users benefits. The sole purpose of these sites is to rob the user credentials. This is often done on the 'search results' page of a search engine.

## 3. A few Anti-phishing techniques

### 3.1. Improving Site Authenticity

The root of the phishing problem is that users are not able to identify if the website is original or fake. Looking at the URL and SSL certificate carefully can really help but not all users have the time or the technical skill to analyze and make the correct judgment.

One method is to personalize the login page for each user. We do the login in two stages. First the user enters only the user-id and not the password. Once user-id is submitted, server returns a page where user gets to see an image which he had selected at time of registration. If the image is matching he supplies the password and all is fine. If the image is not being shown it raises an alert and customer does not provide the password. The phisher does not know which image to display in this intermediate page. Yes it depends on

user being alert. Can a phisher setup a phishing site that acts like a man-in-the-middle and intercept the user-id, send to original site and fetch the image, send image back to user and get the password. Yes, it is technically possible.

#### 3.1.1. Advantages.

- One of the highly secure methods.
- User does not need technical skills.

#### 3.1.2. Disadvantages.

- Man-in-the-middle attack is possible.
- If the image is compromised then phishing is possible.

### 3.2. One-time passwords

The user requires a login-id/static password (often called PIN) and a dynamic one time password for successful login. This one time password is generated on hardware token (or software token) provided to each user. These tokens automatically generate a new one-time-password every 60 seconds.

We are not fighting the real problem here. Users will still get tricked into providing their passwords at the phishing site. But these passwords are only valid for 60 seconds. If the phisher is not able to use it in near-real-time (within 60 seconds) the stolen password is useless. However, as was proven recently, phishers are getting more real-time.

Alternatively, instead of supplying tokens to users, the server can generate the one-time password. Once the login/static-password is validated the one time password can be generated by server and sent via SMS to user's cell-phone. This virtually prevents phishing attacks because attackers can never receive this SMS. But are we saying all users need to have mobile phones and if they are travelling they need to have roaming facility enabled on mobiles every time they need to do Internet Banking? Is the overall cost of transaction increasing?

#### 3.2.1. Advantages.

- For every login a new password is given.
- To prevent phishing, the generated password is sent via SMS to the user's cell-phone.

#### 3.2.2. Disadvantages.

- In case of slow connections, the session password may expire.
- Phishers are getting more real-time.

### 3.3. Having separate login and transaction passwords

It is very relevant for banking and financial sites. This will ensure that even if login password is lost to the phisher, transactions cannot be made. Again we are not saving the users from being victims of phishing. We are just ensuring that even if the login password is lost, attacker can login and see the account details but cannot do something like a fund transfer without knowing the transaction password. If the user has kept both passwords the same then there is no security at all. Alternatively a one-time transaction password can also be generated dynamically by server and sent via SMS to the user.

#### 3.3.1. Advantages.

- For every login a new password is given.
- To prevent phishing, the generated password is sent via SMS to the user's cell-phone.

#### 3.3.2. Disadvantages.

- User needs to remember 2 different passwords, which is sometimes tedious.

### 3.4. User education

It is perhaps the best protection mechanism, but the most difficult one to implement. If we can educate users about how to detect a phishing mail/site and how to securely access the website, a lot of phishing attacks will not succeed. Getting the user's attention to these security tips and advises is challenging. We could put this up on our login page or send it as emails. The method varies depending on the type of business and channels available to reach the user.

#### 3.4.1. Advantages.

- If carried out properly then almost every user can detect the phishing website.

#### 3.4.2. Disadvantages.

- Practically not feasible.

## 4. Conclusion

The world is getting digitalized day after day. Due to this the threats to identities and credentials will always prevail. Our best hope is not to get lured into any kind of fraud. Undoubtedly the above discussed anti-phishing techniques are exceptionally good, but there is always scope for further improvement. This survey paper can be helpful for finding the loopholes and drawbacks of current anti-phishing systems. A comparative study all these systems would definitely help in developing a new system that combines all the advantages and overcomes the drawbacks of these systems.

## 5. References

[1] Phishing Activity Trends Report, 3rd Quarter 2012**,** http://www.antiphishing.org.
[2] Gaurav, Madhuresh Mishra, Anurag Jain "Anti-Phishing Techniques: A Review", ISSN: 2248-9622 www.ijera.com.
[3] Marwaha1, Paresh Marwaha, *Infosys Technologies Limited, India "VISUAL CRYPTOGRAPHIC STEGANOGRAPHY IN IMAGES"*.
[4] James Madison University Infosec, Techreport Department of Computer Science, JMU-INFOSEC-TR-2007-002, "An Overview of Steganography".
[5] http://en.wikipedia.org/wiki/Phishing