MPTPIB-Modern Protection Technique for Phishing in Internet Banking

[1] R.Anantha Krishnan,[2] K.Jebastin,[3] P.John Wesley,[4]D.C.Jullie Josephine
[1,2,3]UG scholar,[4]Professor, Kings Engineering College
[1] Ananthkrish1411@gmail.com, [2] Jebas1995@gmail.com, [3] Johnwesley2916@gmail.com

Abstract— **Phishing is an attempt by an individual or a group to thieve personal confidential information such as passwords, credit card information etc from unsuspecting victims for identity theft, financial gain and other fraudulent activities. The first defense should be strengthening the authentication mechanism in a web application. A simple username and password based authentication is not sufficient for web sites providing critical financial transactions.**

In this paper we have proposed a new approach for phishing websites classification to solve the problem of phishing. Phishing websites comprise a variety of cues within its content-parts as well as the browser-based security indicators provided along with the website. The use of images is explored to preserve the privacy of image captcha by decomposing the original image captcha into two shares that are stored in separate database servers such that the original image captcha can be revealed only when both are simultaneously available; the individual sheet images do not reveal the identity of the original image captcha. Once the original image captcha is revealed to the user it can be used as the password. Several solutions have been proposed to tackle phishing.

I. Introduction

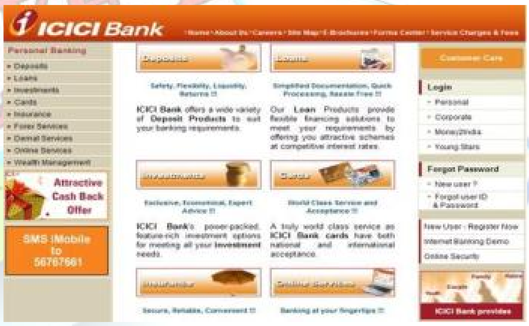
Internet Banking is an easier way to monitor the user's business financial issues.This easy process will also make a common target for Hackers and other online Criminals. As for a security measure, many financial banking websites provides a security image and caption each time when a user logs into the account [1]. The security image and caption are shown to the user on all subsequent logins, and the user is instructed not to log in if she notices that the image or caption are missing or incorrect. This strategy is believed by users to protect them from phishing attacks. If a phishing web site mimics as a real one in all ways except that it does not show the user's chosen security image, which was stored only in original and authenticated banking server.

Examples of well-known banks that use this technology include Bank of America, PNC Bank, and Santander Bank. Bank of America uses an image, an image title, and three challenge questions, together known as the SiteKey [2].Despite the almost ubiquitous use of security images on banking websites, their effectiveness at preventing phishing attacks is uncertain. Previous studies of the effectiveness of security images have reached divergent conclusions: in one, 92% of partici-pants proceeded to log into their real bank accounts even when the security image was absent [3]; in another, 60% of users of an online assignment-submission system noticed missing security images and refused to log in[4].

II Related Work.

Security images are used as one type of visual security indicator. Several studies have shown that visual security indicators, including special toolbars and SSL warnings, are often ineffective [6]. Wu et al. additionally found that many users either do not know about phishing attacks (which security images are intended to prevent), or else do not realize how sophisticated such attacks.To our knowledge there have been only two prior studies, with divergent results, specifically examining the effectiveness of security images. Schechter et al. evaluated several security measures commonly used in online banking, including security images [3].Herzberg and team members examined phishing detection using an assignment-submission system in a university computer-science department [4]. When interactive security images were used—that is, users were required to click on the image during login—almost 60% of users successfully detected phishing when the image was absent.

Our study attempts to address some shortcomings of the two prior studies, while examining not just whether security images are effective but also which factors impact their effectiveness.



Safety, Flexibility, Liquidity, Returns !!!

ICICI Bank offers a wide variety of Deposit Products to suit your banking requirements.

Simplified Documentation, Quick Processing, Hassle Free !!!

Our Loan Products provide flexible financing solutions to meet your requirements by offering you attractive schemes at competitive interest rates.

Exclusive, Economical, Expert Advice !!!

ICICI Bank's power-packed, feature-rich investment options for meeting all your Investment needs.

World Class Service and Acceptance !!!

A truly world class service as ICICI Bank cards have both national and international acceptance.

Secure, Reliable, Convenient !!!

Banking at your fingertips !!!

Fig. 1. ICICI bank website used in the study,

II. Study Methodology

A. Study Procedure

We built a banking website with a similar look and feel to an actual banking website, shown in Figure 1.

To avoid priming, we did not display user about the true purpose of the study; instead, users were told they were to test the website's direct deposit functionality. To complete the study, users were instructed to –report deposits‖ by logging in to their account, clicking a button, and entering a specified amount for a new deposit. During login users entered their user ID, then entered their password on the screen with their security image and caption.

We required users to report five deposits to simulate habituation to security images and captions. To additionally promote realism, users who completed the study re-ceived as compensation the total amount that was –deposited‖ into their accounts. This was similar to that displayed at an actual banking website. The login screen with the security image, caption and the message is shown in Figure 2.

When the participant accessed the site to report the final deposit, the security image and caption were not displayed and were replaced with an ―under maintenance‖ image. The security image and caption were restored for any log-in attempt five minutes or later after that time. This simulates a real-life scenario when the user does not see the security image upon accessing a phished website.

B. Study Conditions

The conditions fall into seven categories. The first category consists of our control condition, while the others explore specific factors that could influence the effectiveness of security images: appearance, interactivity, the ability to customize images, the lack of a caption, and methodological variations. In this paper each participant was assigned to exactly one condition. Users were assigned randomly to one of the first nine conditions. Conditions 10 tested variations in study methodology; users for these were solicited separately (in parallel with soliciting users for the other conditions) because the methodological variations being tested required small changes to the study advertisement.

C) Control Condition.

1) *Control.* Our control condition closely mimics ICICI Bank's implementation of security images. The security image chosen by the participant is shown at 100 pixels high and 100 pixels wide.

Conditions Differing in Appearance. Using these conditions, we seek to explore whether security images with different appearance features make it more likely that a participant will notice that a security image is missing.

2) *Large image.* The chosen security image is shown at 300 pixels high and 300 pixels wide, or nine times larger than in the control.

3) *Blinking image.* Using JavaScript, the security image is made to blink repeatedly in order to draw the user's attention.

Conditions Differing in Interaction. These conditions test whether requiring users to interact with the security image makes it more likely that they will refuse to log in when the security image is missing.

4) *Interactive image.* Users must click on the security image before they can enter their passwords.
5) *Copy random word.* Users must copy a random word placed within the security image before they can enter their passwords.
6) *Copy caption.* Users must copy the caption dis-played with the security image before they can enter their password Condition Differing in Customization. This condition tests whether allowing users to customize their security image increases its effectiveness.

7) *Custom image.* Rather than choosing from a list of available images, users upload an image of their choice.

Condition Differing in Customization, Appearance, and Interactivity. This condition tests whether the simultaneous presence of features present individually in other conditions improves the effectiveness of security images.

8) *Multi-feature.* Users upload an image of their choice. The image blinks continuously (using JavaScript), and the participant must click on it before she can enter her password

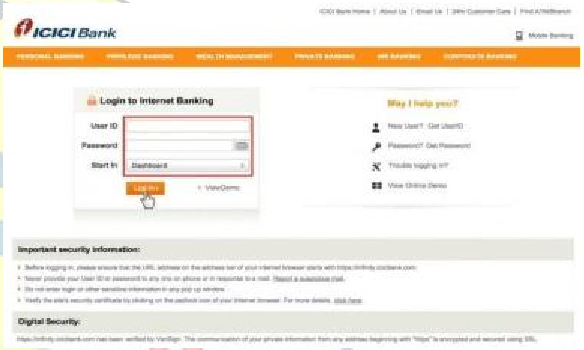


Fig. 2. Login screen

9) *No caption.* Users are not asked to create a caption during account registration, and no caption is shown during login.
10) *Two logins.* Users log in to the account twice, instead of five times as in other conditions. The second time they log in, the security image is removed

III. RESULTS

.

The study was conducted, 345 users signed up for an account on our website. Of these, 293users (85%) completed the entire study by reporting five deposit amounts over five days (or two deposit amounts over two days for users in the two-logins condition). Users who reported at least one deposit amount tended to complete the entire study—only 15 did not finish the study after reporting one or more deposit amounts. For the remainder of this article, we focus on the 293 users who completed the entire study

.

A Sentiment Toward Security Images

At the end of the study, we asked each user to rate her agreement or disagreement with five statements about her security image. We compared the results between conditions –strongly disagree‖, –disagree,‖ and ―neutral‖ responses as one response group and –agree‖ and –strongly agree‖ as another displayed. The remaining 27% users did not do so. We also found no statistically significant difference in the effectiveness of security images based on users' gender, country, major/degree/job, level of education, or security experience

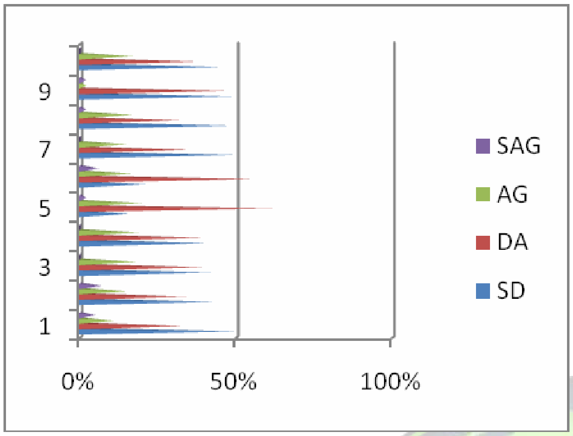


Fig. 3. Users' responses

We received numerous emails from users about the —under maintenance‖ security image, asking us whether or not to log in in the absence of their security image and caption. We replied to such email messages by telling users not to log in, to try again after a few minutes, and to only log in when their correct security image and caption appears. Further discussion of participant emails is found in Section III-C.

B. *Security Image Effectiveness*

Across all conditions, 73% of users entered their passwords when their security image and caption was not displayed. The remaining 27% users did not do so.

We also found no statistically significant difference in the effectiveness of security images based on users' gender, country, major/degree/job, level of education, or security experience.

1."Using a security image as part of the login process was annoying": 5% of users agreed that using the security image was annoying. Across the experimental conditions, agreement varied from 2.2% to 18.2% of users. Users' responses are shown in Figure 3.

Condition *copy-random-word* required the user to type in a random word placed in the image, while the *copy-caption* condition required the user to type in the security caption shown beneath the image each time she logged in to the account. This requires additional effort and slows down the login process, so it was consistent with our expectations that sentiment could be negatively affected.

2) ***"I wish that my bank's website used a similar security image.":*** 42.5% of users in the control condition agreed, and agreement in experimental conditions ranged from 42.4% to 71.8% (*multi-feature* condition). The only statistically significant result was in the *multi-feature*

3) ***"I did not look at the security image before I entered my password.":*** 92.5% in the control condition, and between 84.2% (*large* condition) and 100.0% (*multi-feature* condition) in experimental conditions. Notably, this is a much higher fraction of users than the fraction that declined to log in when the security image was absent. As with the previous statement, the condition that varied most from the control was the *multi-feature* condition. Although this difference was not statistically significant at this sample size, it does suggest that the multiple additional features might have made more users look at the security image before they entered their password.

IV DISCUSSION *A.*

Limitations

As with other studies, the study described in this paper more limitations, including the following.

Our study used fake internet banking accounts, rather than real ones. Although we tried to make the experience as realistic as possible in terms of look and feel, users' motivation to log in within the study would have been different than in a real setting. As with other biases potentially caused by the study framing, this one would likely affect all conditions equally, minimizing its impact on comparisons between condition however, this bias may have influenced the overall finding that security images are ineffective.

In practice, phishing attacks come in many forms. Our methodology involved mimicking one such attack; others could be more (or less) successful, potentially leading to different login rates in the presence of an attack than we observed.

TABLE I. percentage and count of users who entered their password without the security image.

B. *Security Images Are Generally Not Very Effective*

In our control condition, 75% of users entered their passwords even when their security image and caption were not shown. This result differs from the Schechter et al. study which found (in a lab setting) that 92% of users using their own online banking accounts did so.

Our *interactive* condition, in which users were re-quired to click on their security image before logging in, is comparable to the Herzberg and Margulies study [6]. We found that 74% of users in this condition entered their password despite the missing security image; in contrast, only 40% of users in the Herzberg and Margulies study did so.

C. *Effectiveness vs Annoyance*

In general, and perhaps surprisingly, our results suggest that performing additional tasks to log in does not lead to significantly greater effectiveness but can lead to greater annoyance.

For example, users who had to type in a word that appeared in the image or type in the security caption before they could enter their password were not more successful at evading simulated phishing attacks. These users did, on the other hand, experience greater levels of annoyance with the login process, suggesting that adding non-trivial complications or tasks to the login process is not a fruitful avenue for improving the effectiveness of security images and other similar security measures

C. *Evaluating Password Strength*

We examined the strength of the passwords created by the 293 users who completed the entire study by subjecting the passwords to a password-cracking algorithm.

The key to protecting your Internet banking account is protecting your password. Using a strong password -- one that contains mixed-case letters, numbers, and even symbols if the bank allows it -- will decrease the likelihood of a hacker cracking the password and gaining access to your account. You should also ensure that the password to access your company's accounts is not the same as any other password you use, since not every site maintains the same level of security a bank does. If a hacker manages to steal a password from an insecure site, he can access any account that password unlocks. Passwords were cracked in a manner that simulated an attacker with moderate knowledge of currently available password-cracking tools.

D. *Effectiveness vs Noticeability*

Interestingly, the *multi-feature* condition, where participants defined the security image, the image blinked, and users had to click on the image, proved no more effective than conditions with much subtler image effects and fewer attention-grabbing features. This is despite the fact that more users in the *multi-image* condition stated that they looked at the security images before they entered the password compared to the control condition. This highlights that there is a gap between reported noticeability and the likelihood of logging in when the security image was absent, which we also observed across conditions.

E. *Additional Interaction Doesn't Improve Effectiveness*

None of the interactive conditions, in which users had to click or type something related to the security image before they could enter a password, significantly affected the effectiveness of the security image. This result diverges from Herzberg and Margulies [6].

In the *interactive* condition, users might have clicked on the image without noticing whether the image was correct. In the two *copy* conditions, users reported more annoyance than in the control condition, suggesting an increased awareness of the security image. However, the added inconvenience may have made users glad to find the site —under maintenance," allowing them to proceed more quickly.

F. *Customization Does Not Improve Effectiveness*

Also surprisingly, users who uploaded their own im-ages to use as their security image—instead of choosing from a list of images provided by the website—were not significantly more effective at noticing the absence of a security image.

G. *Habituation, Motivation, and Priming Have Little Impact*

To the extent that these factors were exposed by our study, habituation, the financial compensation to users, and the amount of security priming users received did not significantly affect users' ability to notice and effectively react to missing security images.

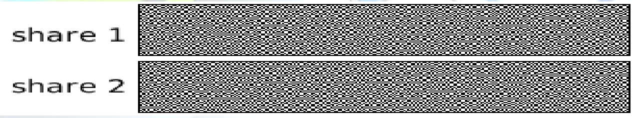
V Proposed Methodology

To prevent and Detect the phishing website,we are proposing a technique called Visual Cryptography. This technique is based on the Anti-Phishing Image processing and validation scheme. It will prevents password and other confidential information of the user from phishing websites before login in to the user account.

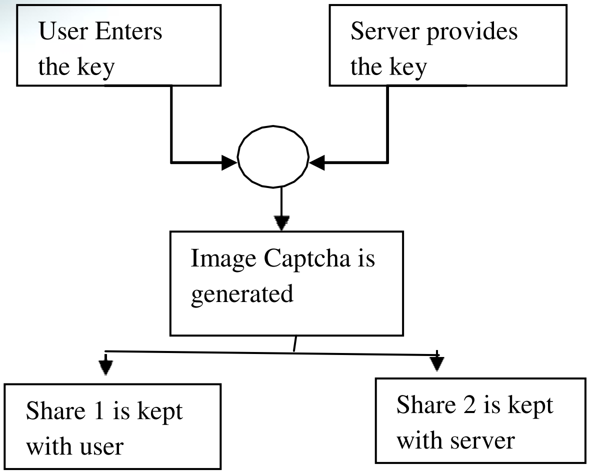
The proposed approach can be divided into two phases:

1.REGISTRATION PHASE

In the registration phase, a key string (secret code) is asked from the user at the time of registration for the secure website. The key string can be a combination of alphabets and numbers to provide more secure Registration. This string is concatenated with randomly generated string in the server and an image captcha is generated. The image captcha is divided into two shares such that one of the shares is given to the user and the other share is kept in the authenticated server. The user's share is sent to the user for later verification during login phase. The image captcha is also stored in the actual database of any authenticated website as confidential data. After the complete registration, the user can change the key string when it is needed. The shares are displayed in fig.4

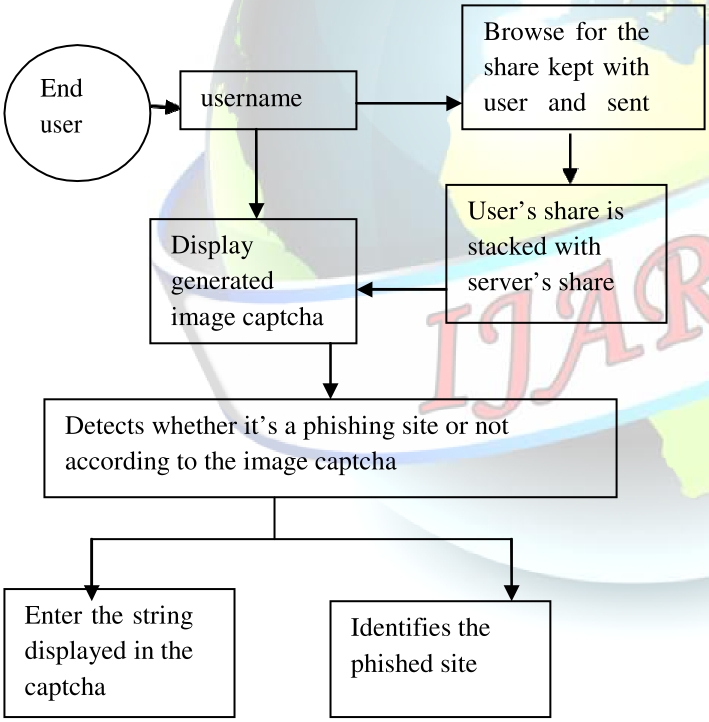


The Registration is illustrusted as a DFD fig.5


User Enters the key
Server provides the key
Image Captcha is generated
Share 1 is kept with user
Share 2 is kept with server

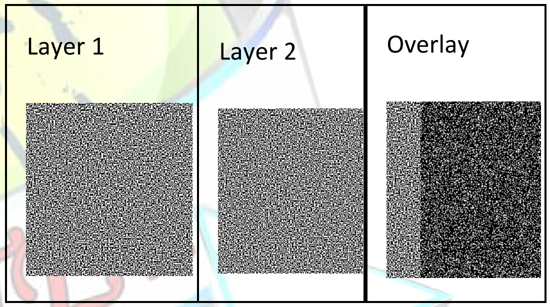
2.LOGIN PHASE

In the Login phase first the user is prompted for the username (user id).Then the user is asked to enter his share which is kept with him. This share is sent to the server where the user's share and share which is stored in the database of the original website, for each user, is stacked together to produce the image captcha. The image captcha is displayed to the user .Here the end user can check whether the displayed image captcha matches with the captcha created at the time of registration. The end user is required to enter the text displayed in the image captcha and this can serve the purpose of password and using this, the user can log in into the website. Using the username and image captcha generated by stacking two shares one can verify whether the website is genuine/secure website or a phishing website and can also verify whether the user is a human user or not.Figure.4 can be used to illustrate the login phase.


End user
username
Browse for the share kept with user and sent
User's share is stacked with server's share
Display generated image captcha
Detects whether it's a phishing site or not according to the image captcha
Enter the string displayed in the captcha
Identifies the phished site

VI Future Enchancement

Material provided in the following sections is for informational purposes only. The selection and use of any technique should be based upon the assessed risk associated with a particular electronic banking product or service.Visual Cryptography is a special encryption technique to hide information in images in such a way that it can be decrypted by the human vision if the correct key image is used.It is impossible to retrieve the secret information from one of the images. Both transparent images or layers are required to reveal the information. The easiest way to implement Visual Cryptography is to print the two layers onto a transparent sheet. When the random image contains truly random pixels it can be seen as a one-time pad system and will offer unbreakable encryption. In the overlay animation you can observe the two layers sliding over each other until they are correctly aligned and the hidden information appears. To try this yourself, you can copy the example layers 1 and 2, and print them onto a transparent sheet or thin paper. Always use a program that displays the black and white pixels correctly and set the printer so that all pixels are printed accurate (no diffusion or photo enhancing etc). You can also copy and paste them on each other in a drawing program like paint and see the result immediately, but make sure to select transparent drawing and align both layers exactly over each other.



Shares

REFERENCES

[1] J. Kirk, –Study: Users ignore bank security features,‖ *Computerworld*, Feb. 2007, http://www.computerworld.com/s/article/9010283/.

[2] Bank of America, –SiteKey FAQs,‖ https://www.bankofamerica.com /privacy/faq/sitekey-faq.go, 2013.

[3] S. Schechter, R. Dhamija, A. Ozment, and I. Fischer, –The emperor's new security indicators: An evaluation of website authentication and the effect of role playing on usability studies,‖ in *Proceedings of the 28th IEEE Symposium on Security and Privacy*, Berkeley, CA, USA, 2007, pp. 51–65.

[4] A. Herzberg and R. Margulies, –Forcing Johnny to login safely,‖ in *Proceedings of the 16th European Symposium on Research in Computer Security*, Leuven, Belgium, 2011, pp. 452–471.

[5] Christo Ananth, H.Anusuya Baby, "Encryption and Decryption in Complex Parallelism", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Volume 3, Issue 3, March 2014,pp 790-795

[6] J. Sunshine, S. Egelman, H. Almuhimedi, N. Atri, and L.F. Cranor, –Crying wolf: An empirical study of SSL warning effectiveness,‖ in *Proceedings of the 18th USENIX Security Symposium*, Montreal, Quebec, Canada, 2009, pp. 399–432.