Yahoo!'s Sign-in Seal and current anti-phishing solutions

Naveen Agarwal, Scott Renfro, Arturo Bejar
Yahoo! Inc.

Abstract

We examine Yahoo!'s Sign-in Seal and some of the considerations that affected the design. Unlike solutions like SiteKey which are tied to a user's account, Yahoo!'s sign-in Seal is tied to a browser. We have found "Rusty's Axioms" to be useful for analyzing the security of both anti-phishing solutions and also other user interaction with our site.

1. Introduction

Phishing is a significant risk facing internet users today [1,2].

Yahoo! users may be phished of their username and password so that a phisher can look for valuable information in their account. To help protect Yahoo! users and combat phishing, Yahoo! developed Sign-in Seal.

2. Brief overview of the Sign-in Seal

Yahoo! Sign-in Seal is a feature that allows users to personalize a sign-in page with an image of their choice. Unlike SiteKey [5], the personalization is tied to the browser/computer and not to a specific user account. This is a critical distinction that causes the two solutions to have quite different properties.

When signing into Yahoo!, a user receives a "Call to Action" (CTA) prompting them to personalize their sign-in page. This appears in the form of an image titled "prevent password theft" adjacent to the Yahoo!ID, password fields of the sign-in page.

The user can either create their Sign-in Seal from an image they upload or from text they provide. The text background and border color is randomly selected, although the user has the option to change the color. If they choose to upload an image, it is resized in preparation for storage and display while if they choose to enter text, an image is created from the provided text.

After the image is prepared, it is displayed in "preview" form. The user can then make further changes. When they are happy with their seal, they save it.

When the user saves the seal, they are reminded that the seal is set up only on the current computer and that they should create a seal for other computers they use. We save information in a cookie that lets us display the browser's seal and also cache that information via other mechanisms available in the browser (e.g., Flash Shared Object, Internet Explorer Persistent User Data [9]).

Sign-in page with a seal.

The user is then taken to a sign-in page where the seal is displayed prominently inside the login box. At any time in the future, someone using that same browser/computer can change the Sign-in Seal.

3. Design Considerations

Prior to designing the Sign in Seal, we identified a set of three axioms that are central to the analysis of anti-phishing solutions. We named these "Rusty's Axioms." [1]

1. Anything a phisher can see, he can spoof.

The Sign-in Seal is personalized to every browser/computer based on an image or text selected by the user. Only the users of a given browser/computer see the Sign-in Seal associated with that browser/computer. The variety in images and text selected by users makes spoofing the Sign-in Seal harder than spoofing a small set of stock images or phishing indicators.

2. Anything a user knows, he can reveal to the phisher.

The display of the Sign-in Seal is based on the cookies that are set in the browser. Unlike passwords and account recovery information, an average user can not easily give their cookies to a phisher. Of course it's still important to protect against browser or page flaws (e.g., cross-site scripting) that may leak this information without user involvement.

3. Any phishing solution is only as good as its first step.

The user is not required to enter any credentials (userid, password etc) to either setup or view the Sign-in Seal. There is a risk of a user getting phished by solutions that require the user to authenticate with information they know before display because the phisher can spoof such pages. The Sign-in Seal eliminates this problem, as it is the site that needs to authenticate itself to the user.

A common distinction amongst anti-phishing solutions is how users associate a new computer. Sign-in Seal treats the new computer use case the same as first-time setup, encouraging users to ensure they're actually at Yahoo! and setting up a new computer before completing the process.

We also identified a set of business and functional requirements early in the process:

1. Sign-in should remain a one-step process.

Yahoo! has millions of users who login on a daily basis and they are accustomed to the current process. It was important to keep sign-in a one-step process.

2. Existing user flows should continue to work with or without the new solution.

Yahoo! offers a lot of services to its users and users sign-in to Yahoo! in multiple flows (e.g. messenger, other clients, country specific processes). It is not practical to change all the processes at once.

3. Users should easily be able to sign in from café's, mobile phones.

[1] Rusty's Axioms are named after Rusty Shakleford, the pseudonym often employed by Dale Gribble, the paranoid character in the TV cartoon King of the Hill [8]

A lot of users (especially internationally) access Yahoo! services through public computers in cafes or through mobile phone. These users can not be expected to go through a special setup before signing in. All these users should continue to be able to sign-in normally even though they do not have the Sign-in Seal.

4. Sign-in Seal image URL should change frequently.

The Sign-in Seal URL is valid only for a short time. If the URL to the Sign-in Seal image is static then an attacker with access to the user's browser history, browser cache can later replay that same image embedded in a malicious page. Additionally, it may be possible to convince a user to reveal their Sign-in Seal image URL. Expiring the URL limits the effectiveness of these attacks.

5. The Sign-in Seal and any pages containing it cannot be framed.
Any page that displays Sign-in Seal includes frame busting code. Allowing the Sign in Seal to be framed would allow an attacker to integrate the Sign-in Seal into a malicious page.

Sign-in Seal is customized with the picture or the text that a user provided rather than more generic stock photographs. We expect that the longer a user has a given image of their own selection, the more their affinity for that image will grow.

4. Comparisons

Current anti-phishing solutions broadly fall into these two categories.

1. Site Badges

Site Badges, like Passmark SiteKey and Yahoo! Sign-in Seal, allow users to customize their sign-in page in some way. The intent is that this better authenticates the site to the user.

Passmark SiteKey is customized to each site that deploys the solution. Setup occurs after a user has authenticated and involves the user providing some text and selecting one of the stock images.
The image and text are associated with the user's browser/computer as well as their account.

On future sign-in pages viewed on the same browser/computer, the user's image and text is displayed after the user enters the user id. When the user signs in from a different computer, they are asked to provide some account information (similar to account recovery) so that their image and text associated with their account can be associated with that browser/computer.

In contrast, Yahoo! Sign-in Seal is only associated with a browser/computer and not with a user's account. Setup does not require any account information – even when setting up on different computers. Additionally, the Sign-in Seal is based on a personal picture instead of a stock photographs, which is intended to increase affinity for the image. Users of shared computers may choose a picture that is meaningful to the entire group (e.g., a picture of the family pet). The Sign-in Seal is not offered on known-public computers.

2. Phishing indicators

Various toolbars and browser add-ons highlight phishing and legitimate sites. These solutions typically rely on heuristics, blacklists and whitelists. This solution is not generally customized to a particular site. These indicators may help protect a user for any site on the Internet.

Previous studies [3,4] have evaluated various solutions and found that most users pay little or no attention to security/phishing indicators. In addition, there may be privacy issues as well as false positives in the blacklist and false negatives in the white list.

5. Sign-in Seal effectiveness

We have anecdotal data that suggests that users develop a strong affinity for their images over time and that the Sign-in Seal can be quite effective for some users. Unfortunately, we have not yet been able to design an objective study that evaluates Sign-in Seal's real world performance. We suspect that the effectiveness cannot be accurately measured in a lab because it is hard to replicate the effect of growing affinity for personal images over time.

Additionally, because the Sign-in Seal is not associated with a user, we cannot tell whether a user who was phished was phished while using a browser/computer that has a Sign-in Seal configured.

We have heard from our users that the Sign-in Seal has been able to help them avoid being phished.

From a user:
"I received this in my Yahoo! messenger today. *Text and a link (removed).*

Luckily I have been using the sign-in-seal so when I clicked on the link I knew right a way that this wasn't the real thing. I've never been phished like this before so I thought that I would bring this to your attention."

Conclusion

Phishing is an industry-wide challenge with evolving threats and countermeasures. Due to the social and human components, there are no completely effective solutions. Only through learning from our shared experiences can we hope to better protect Internet users. We have found "Rusty's Axioms" useful in analyzing the Yahoo! Sign-in Seal and several other Yahoo! features.

References

[1] Anti-Phishing Working Group, *Phishing Activity TrendsReport March 2005*, http://www.antiphishing.org/reports/apwg_report_february_2007.pdf.

[2] Anti-Phishing Working Group, APWG Phishing Archive, http://anti-phishing.org/phishing_archive.htm.

[3] R. Dhamija, J. Tygar, and M. Hearst. Why Phishing Works. In *Human Factors in Computing Systems (CHI 2006)*, Quebec, Canada, Apr. 22–27, 2006.

[4] The Battle Against Phishing: Dynamic Security Skins, Rachna Dhamija and J. D. Tygar, in *Proceedings of the Symposium on Usable Privacy and Security (SOUPS)*, July 2005

[5] Bank of America. SiteKey: Online Banking Security. http://www.bankofamerica.com/privacy/sitekey/index.cfm.

[6] Yahoo! Inc. What is a sign-in seal? - Yahoo! Account Security. http://help.yahoo.com/l/us/yahoo/security/phishing/phishing-110140.html.

[7] Yahoo! Inc. Yahoo! Personalized Sign-In Seal. https://protect.login.yahoo.com/.

[8] Dale Gribble - Wikipedia. http://en.wikipedia.org/wiki/Dale_Gribble.

[9] Persisting Session Information. http://msdn2.microsoft.com/en-us/library/ms533015.aspx.