PHISHING

NAVEEN AGARWAL, SCOTT RENFRO,
and ARTURO BEJAR, YAHOO!

Phishing is a significant risk facing Internet users today.[1,2] Through e-mails or instant messages, users are led to counterfeit Web sites designed to trick them into divulging usernames, passwords, account numbers, and personal information. It is up to the user to ensure the authenticity of the Web site.

Browsers provide some tools (e.g., URL, SSL indicators, and optional toolbars), but these are limited by at least three issues:

- Users do not know which indicators are trustworthy.
- The browser indicators can be easily spoofed (e.g., by including them in the page or painting over them with chromeless windows).
- Users do not look outside their primary areas of interest. Internal eye-tracking studies done by Yahoo! on login pages showed that users see only the small rectangle bounding the username and password fields of the page.

One approach to overcoming this problem is to educate users to look outside their existing comfort zone and examine existing browser indicators. Another approach, which is used by the Yahoo! sign-in seal, is to place a reliable indicator within the area users already see.

OVERVIEW OF THE SIGN-IN SEAL

The Yahoo! sign-in seal is a feature that allows users to personalize a sign-in page with an image of their choice.[3,4]

Unlike the Passmark SiteKey used by Bank of America,[5] the personalization is tied to the browser/computer and not to a specific user account. This is a critical distinction that gives the two solutions quite different properties.

When signing in to Yahoo!, users who have not already personalized their sign-in page receive a CTA (call to action) prompting them to do so. This appears in the form of an image titled “prevent password theft” adjacent to the login fields of the sign-in page.

The user can create a sign-in seal from either an uploaded image or text the user provides. The text background and border colors are randomly selected, although the user has the option to change the color. If the user chooses to upload an image, it is resized in preparation for storage; if the user chooses to enter text, an image is created from the provided text. The prepared image is stored on Yahoo!’s image servers where it receives a unique ID. The image can be accessed only with a valid token that is time-limited and protected by a secret shared between the login and image servers.

After the image is stored, it is displayed in preview form. The user can make additional changes, then save it. This seal is specific to the computer being used and is not associated with the user’s account. As a result, this computer’s sign-in seal does not appear on other computers, unless a user happens to set up an identical-appearing

FORBIDDEN

Current anti-phishing technologies prevent users from taking the bait.

seal—even then, the two seals, though they appear to be identical, would be unrelated.

Since it may not be obvious that a seal is specific to a particular computer, the user is reminded while saving the seal that it is set up only on the current computer and that the user must create seals for other computers. Yahoo! saves the encrypted unique ID in a cookie that lets the login servers later generate an image URL that contains a valid token. This image URL is embedded in the sign-in page, causing the image to be fetched from the image servers. Because a user may clear cookies without intending to, thus removing the sign-in seal, Yahoo! also caches that information via other mechanisms available in the browser (e.g., Flash Shared Object, Internet Explorer Persistent User Data[6]). This cached information is used to display the sign-in seal only when cookies are missing. There is a way for users to remove their seals through the setup page. Although it's possible for these caches to get out of sync, they are not frequently used; thus, syncing them periodically is usually sufficient.

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.

DESIGN CONSIDERATIONS

Prior to creating the sign-in seal at Yahoo!, we identified a set of three axioms that are central to the analysis of anti-phishing solutions. We called these Rusty's Axioms, named after Rusty Shackleford, the pseudonym often employed by Dale Gribble, the paranoid character in the TV cartoon *King of the Hill*.

Axiom 1: Anything phishers can see, they can spoof. If a generalized indicator is used to give the user information about the site/Web page, a phisher can easily duplicate that indicator and show it to the user. Examples include the lock icon, any other indicator in the browser chrome, or indicators from the toolbar. A number of studies have shown that most users don't pay attention to these indicators.[7,8]

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 more difficult than spoofing a small set of stock images or phishing indicators.

Axiom 2: Anything users know, they can reveal to phishers. The number of secrets held by users to protect their accounts should be limited since users can and will be tricked into leaking those secrets. All password-based systems are at risk of the user divulging the password. Both the text-based seal and systems based on a small number of images may be at small risk of phishing (the actual text of the seal could be phished). If the display of a security indicator is based on the user providing some secret information, then the solution is at risk.

Since the Yahoo! sign-in seal does not allow transfer of the seal across computers, no additional information, beyond the seal itself, can be phished. The display of the sign-in seal is based on the cookies that are set in the browser. Unlike passwords and account recovery information, average users cannot easily give their cookies to phishers. 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.

Axiom 3: Any phishing solution is only as good as its first step. The disadvantage of any solution is that normally the first step is a spoofable operation. Solutions should limit the number of spoofable operations that require users to divulge secrets.

The sign-in seal does not require users to enter any credentials (user ID, password, etc.) either to set up or to view the seal. There is a risk of users getting phished by solutions that require them to authenticate with information they know before display because phishers 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 among anti-phishing solutions is how users associate a new computer. Setting up the sign-in seal on a new computer does not require users to reveal secrets (whereas a SiteKey solution requires secret information to use a new computer). The sign-in seal treats the new computer use case the same as first-time setup, encouraging users to ensure they're actually at Yahoo! (by examining the URL to ensure it begins with https://login.yahoo.com/ and/or by manually typing yahoo.com into the browser's location bar) and setting up a new computer before completing the process.

We also identified a set of business and functional requirements early in the design of the sign-in seal:

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

Existing user flows should continue to work with or without the new solution. Yahoo! offers many services to its users, who sign in to Yahoo! in multiple flows (e.g., messenger, other clients, country-specific processes). Changing all the processes at once would not be practical.

Users should be able to sign in easily from cafés or mobile phones. Many users (especially internationally) access Yahoo! services through public computers in cafés or through mobile phones. These users cannot be expected to go through a special setup before signing in. They should continue to be able to sign in normally, even though they do not have the sign-in seal.

The sign-in seal image URL should change frequently. Although it's not visible to the user, the sign-in seal URL is valid only for a short time and changes frequently. If the URL to the sign-in seal image does not change frequently, then an attacker with access to the user's browser history or browser cache can later replay that same image embedded in a malicious page. Additionally, with long-lived image URLs, it might be possible to convince users to reveal their sign-in seal image URLs. Expiring the URL limits the effectiveness of these attacks.

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

The sign-in seal is customized with a picture or text that a user provides rather than with generic stock photographs. We expect that the longer a user has a given image of his or her own selection, the more the user's affinity for that image will grow.

COMPARISONS

Current anti-phishing solutions fall into two broad categories: site badges and phishing indicators.

Site badges. Site badges, like the Passmark SiteKey and the Yahoo! sign-in seal, allow users to customize their sign-in pages. The intent is better authentication of the site to the user.

The 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 the user's account.

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

In contrast, the Yahoo! sign-in seal is associated only 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—which limits the effectiveness of an attack that prompts users for the first-tier authentication data that reveals their images. Additionally, the sign-in seal is based on a personal picture instead of stock photographs, which is intended to increase affinity for the image. Users of shared computers may choose an image 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.

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 and should help protect users on any Internet site.

Previous studies have evaluated various solutions and found that most users pay little or no attention to security/phishing indicators.[9,10] In addition, there may be privacy issues, as well as false positives in the blacklist and false negatives in the whitelist.

SIGN-IN SEAL EFFECTIVENESS

Anecdotal data suggests that users develop a strong affinity for their images over time and that the Yahoo! sign-in seal can be quite effective for some users. Unfortunately, we have not yet been able to design an objective study that evaluates the sign-in seal's real-world performance. It is unlikely that the effectiveness can be accurately measured in a lab because it is difficult to replicate the effect of a growing affinity for personal images over time.

Additionally, because the sign-in seal is not associated with a user, it is impossible to tell if a user whose account was compromised was phished while using a browser/computer that has a sign-in seal configured.

We have heard from Yahoo! users, however, that the sign-in seal has helped them avoid being phished. For

example, this came 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 away 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."

POSSIBLE LIMITATIONS

The sign-in seal solution relies on users to notice the seal when signing in. If users ignore the fact that their seal is not displayed and still sign in, they are vulnerable to phishing. To mitigate the issue, the seal is displayed inside the login box where they enter information. The seal is also personalized so users develop an affinity to it. Yahoo! has started issuing authentication credentials that are valid for two weeks so users sign in less frequently, making the sign-in process a special event. In the past users had to sign in on a daily basis; this made them accustomed to typing their passwords without much thinking. As users get used to signing in every two weeks, they may be more likely to notice if they are asked to sign in more frequently.

One of the main issues with this solution is related to clearing the cookies. If users upload an image to Yahoo! servers, they expect it to be persistent and not just go away by clearing cookies and private data. We have tried to overcome this issue by also caching the information via other mechanisms available in the browser (e.g., Flash Shared Object, Internet Explorer Persistent User Data[11]). Internet Explorer 7 and Firefox 2.0 provide users an easy way to clear all private data. This leads to the loss of users' seals, forcing them to set up the seals again.

Another issue with the sign-in seal is related to user education. The SiteKey solution is frequently confused with this solution, and some users think (incorrectly) that their seals are tied to their accounts. They expect that the same seal should be displayed on all the computers they use, similar to SiteKey. We have tried to address this by clearly messaging users when they set up their seals.

LEARNING FROM EXPERIENCE

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

REFERENCES

1. Anti-Phishing Working Group. 2007. *Phishing Activity Trends Report* (March); 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. Yahoo! Inc. What is a sign-in seal? Yahoo! Account Security; http://help.yahoo.com/l/us/yahoo/security/phishing/phishing-110140.html.
4. Yahoo! Inc. Yahoo! personalized sign-in seal; https://protect.login.yahoo.com/.
5. Bank of America. SiteKey: Online banking security; http://www.bankofamerica.com/privacy/sitekey/index.cfm.
6. Persisting Session Information; http://msdn2.microsoft.com/en-us/library/ms533015.aspx.
7. Dhamija, R., Tygar, J., Hearst, M. 2006. Why phishing works. In *Human Factors in Computing Systems* (CHI 2006), Quebec, Canada (Apr. 22–27).
8. Dhamija, R., Tygar, J. 2005. The battle against phishing: Dynamic security skins. In *Proceedings of the Symposium on Usable Privacy and Security* (July).
9. See reference 7.
10. See reference 8.
11. See reference 6.

LOVE IT, HATE IT? LET US KNOW

feedback@acmqueue.com or www.acmqueue.com/forums

NAVEEN AGARWAL spends most of his time coming up with innovative ways to protect users. **SCOTT RENFRO** earns his keep by sniffing out and fixing security flaws in large applications, including his own. **ARTURO BEJAR** earns his living being paranoid and making other people paranoid. All the authors work for Yahoo!.