An Evaluation of Extended Validation and Picture-in-Picture Phishing Attacks

Collin Jackson[1], Daniel R. Simon[2], Desney S. Tan[2], and Adam Barth[1]

[1] Stanford University, Stanford, CA
{collinj, abarth}@cs.stanford.edu
[2] Microsoft Research, Redmond, WA
{dansimon, desney}@microsoft.com

Abstract. In this usability study of phishing attacks and browser anti-phishing defenses, 27 users each classified 12 web sites as fraudulent or legitimate. By dividing these users into three groups, our controlled study measured both the effect of *extended validation* certificates that appear only at legitimate sites and the effect of reading a help file about security features in Internet Explorer 7. Across all groups, we found that *picture-in-picture* attacks showing a fake browser window were as effective as the best other phishing technique, the *homograph* attack. Extended validation did not help users identify either attack. Additionally, reading the help file made users more likely to classify both real and fake web sites as legitimate when the phishing warning did not appear.

1 Introduction

Paranoia surrounding fraud remains a barrier to using online commerce for many consumers. The padlock encryption symbol used by browsers to indicate HTTPS encryption is often misunderstood, does not appear on the login pages of many legitimate sites, and does not provide users with a reliable mechanism for distinguishing fraudulent sites from real sites. Attackers have increasingly exploited this weakness with *phishing* attacks, sending email to victims enticing them to visit a fraudulent copy of a web site [1]. Over 26,000 unique phishing attack web sites were reported to the Anti-Phishing Working Group in August 2006 [2]. These attacks have cost banks and card issuers billions of dollars [3].

In response, the certificate authority industry has developed a new technology, tentatively named *extended validation* or *high assurance* certificates [4]. Unlike normal certificates, which indicate only that the owner controls a particular domain name, extended validation certificates also attest to the identity of a legitimate business. Internet Explorer 7 indicates the presence of these certificates by turning the address bar green and providing more information about the certificate owner, as shown in Fig. 1.

Our study measured the effect of this new technology on users determining whether or not a page is legitimate. The participants were divided into three groups: one group was trained in the use of green address bars (indicating extended validation certificates that appear only at legitimate sites), one group saw

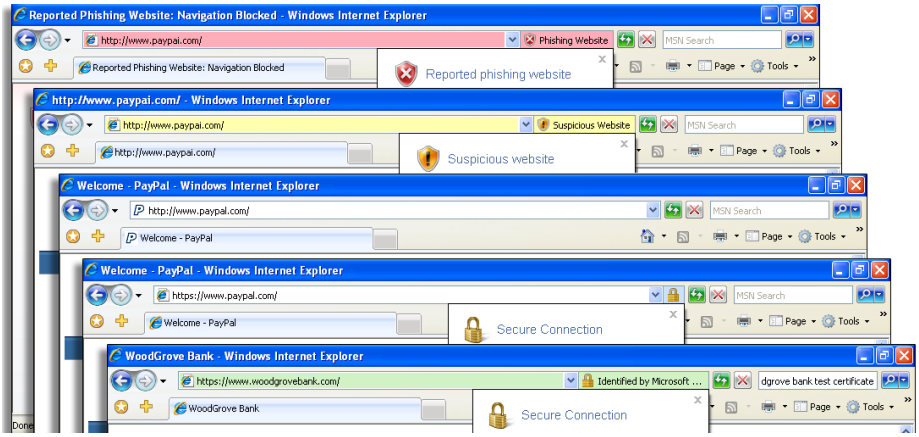

Fig. 1. Phishing, suspicious, HTTP, HTTPS, and extended validation indicators.

extended validation indicators but received no training, and a control group was not shown extended validation indicators at all. After familiarizing themselves with two online financial web sites, the participants were shown a series of pages claiming to be those web sites and were asked to classify the pages as legitimate or fraudulent. We compared user responses at the real site, *homograph* [5] sites with similar domain names, and *picture-in-picture* sites that show a fake browser window. Our key findings are:

- Picture-in-picture attacks were as effective as homograph attacks.
- Extended validation did not help users defend against either attack.
- Extended validation did not help untrained users classify a legitimate site.
- Training caused more real and fraudulent sites to be classified as legitimate.

Participants were trained by reading a portion of the Internet Explorer 7 help file that describes both the phishing filter and extended validation features. Our study provides only an upper bound on the efficacy of these indicators because study participants were explicitly instructed to classify sites.

2 Related Work

2.1 Phishing warnings

One approach to protecting users from phishing attacks is to detect when the browser arrives at an untrustworthy page and warn the user. If the warnings are accurate, and the user heeds them, the phishing page is not able to obtain any information from the user [6]. This approach has been implemented commercially in the form of security toolbars [7–9]. These toolbars rely on an up-to-date blacklist, and the composition of the blacklist has a major effect on

the accuracy of the toolbar [10]. Although it is difficult for these phishing filters to attain perfect accuracy, they have nonetheless become popular and are now integrated into most major browsers, including Internet Explorer 7, Mozilla Firefox 2, Netscape 8, and Opera 9.1.

2.2 Positive trust indicators

Because it is difficult to build a perfect blacklist of phishing sites, a complementary approach is to show a positive trust indicator, indicating that it is safe for the user to proceed. The lock icon in browsers, which indicates the presence of SSL/TLS encryption, does not ensure the site is trustworthy. Certificate authorities issue domain-validated certificates to anyone who can demonstrate domain ownership by receiving emails addressed to that domain name. The lock icon is frequently ignored by users [11], not present when the login form first appears [12], and displayed on phishing sites that use encryption [13].

Extended validation, which turns the address bar green in Internet Explorer 7, also does not guarantee that the site is "safe" to do business with or that it complies with applicable laws. However, extended validation does provide more accountability for the domain owner, which must be a legally incorporated entity and have a registered office. Unlike regular certificates, extended validation certificates cannot be issued to general partnerships, unincorporated associations, sole proprietorships, and individuals [14].

One disadvantage of positive security indicators is that users have to look for them. In actual usage scenarios, security is rarely a user's primary goal [15]. Anti-phishing tools that provide only neutral or positive information are easier to ignore than phishing warnings [16]. Positive security indicators can also mislead users of a legitimate web site that has been hijacked by an attacker using web vulnerabilities such as cross-site scripting.

2.3 Trusted user interfaces

Browser security indicators (particularly positive trust indicators) are often prone to user interface spoofing attacks. In an overlapping window environment with a predictable window appearance, an attacker could convince the user that the contents of a web page, under attacker's control, is actually part of the browser [12]. An example picture-in-picture attack with a fake browser window is shown in Fig. 2. User interface spoofing attacks can be foiled using secret images [17] or an unpredictable browser appearance [18, 19] that the attacker cannot spoof. These schemes rely on the assumption that the user will not proceed if the trusted image is not present. One of the sites used in our study, Bank of the West, has announced plans to adopt a trusted image scheme in the future.

2.4 Other authentication approaches

Most commercial web sites rely on a relatively weak form of password authentication: the browser simply sends a user's plaintext password to a remote web

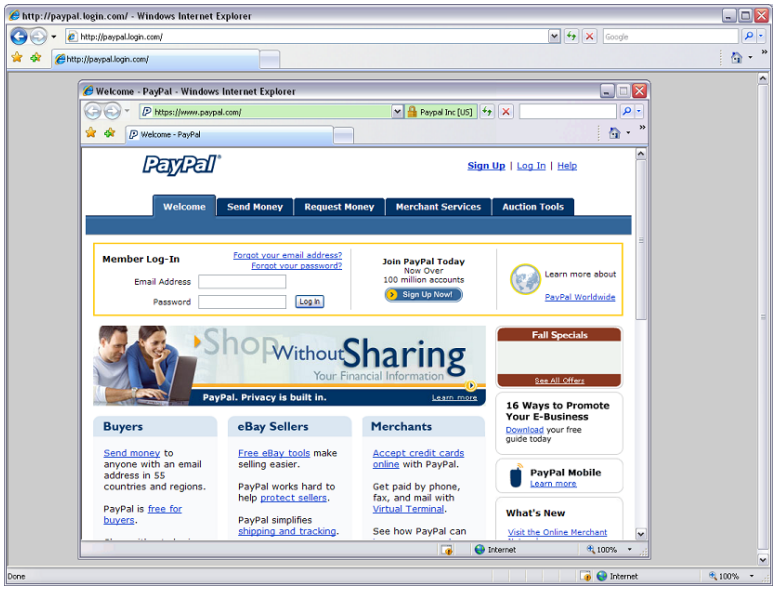

Fig. 2. Picture-in-picture attack. Both the outer (real) window and the inner (fake) window are focused at the same time. The inner window cannot be maximized.

server using SSL/TLS. Unfortunately, the remote web server is not limited to verifying that the password is correct; it can also use the password to log in elsewhere. Although techniques such as SSL/TLS with client-side certificates [20] can solve the password theft problem, they are difficult to use and have not yet become widespread. Newly proposed systems make client certificates more usable by employing trusted devices [21] and operating system support [22]. For users who rarely change computers, a long-lasting cookie can be used as a convenient alternative to client certificates, usually as a second factor of authentication [17].

Another approach to the password theft problem is a password manager that automatically generates a unique password for each site, ensuring that the user's password at that site cannot be used anywhere else [23]. These solutions can be vulnerable to picture-in-picture user interface spoofing, so it is important to provide a trusted path to prevent the master password from being compromised [24–26]. The trusted path must also be easy to use [27].

Preventing password theft does not protect victims if the phishing attacker does not try to steal the user's password, but instead asks the user directly for other sensitive personal information, such as a social security number.

3 Study Design

Study participants first familiarized themselves with two web sites. One group then received training in the address bar security features, whereas two other

groups did not. Participants in all three groups were then asked to classify 12 web sites as legitimate or fraudulent.

3.1 Familiarization

At the beginning of the study, the participants were provided with a computer equipped with the Internet Explorer 7 web browser and instructed to familiarize themselves with two legitimate web sites, PayPal and Bank of the West, presented in a random order. The familiarization step provided participants an opportunity to learn about the look and feel of the real sites before being asked to classify the test sites as legitimate or fraudulent, and, more importantly, gave them an opportunity to learn whether the extended validation security indicator is normally active when using the real site. The participants were randomly divided into three groups who were presented with different experiences:

- **Trained Group.** The trained group was shown extended validation security indicators at each of the real sites. Before the familiarization step, the trained group was also asked to read excerpts from the Internet Explorer help file explaining the security features of the address bar in Internet Explorer 7, including both the phishing filter and extended validation.
- **Untrained Group.** The untrained group was shown extended validation security indicators at each of the real sites, but received no explanation of the meaning of the green address bar.
- **Control Group.** The control group did not see any extended validation indicators during the familiarization step. They received a modified version of the tasks that did not include any extended validation indicators.

Participants in each group were given a fake username and password to use at each site and were instructed to log in when they were ready to continue. The tasks began after the participants had successfully logged in to both sites with the provided username and password.

3.2 Tasks

Once the familiarization step was complete, participants were directed to a web page containing links to 12 web sites in a random order. The link was identified only by a number, preventing the participants from knowing the nature of the site to which they were connecting. They were asked to respond to this prompt:

> *Imagine you receive an email message that asks you to click on the link shown here. Imagine that you decide to click on the link to see if it is a legitimate web site or a "spoof" (a fraudulent copy of that web site).*

The web sites shown were divided into the following categories:

- **Real site.** A site shown in the familiarization step. Sometimes the link would open in a new window, and at other times it would open in the current browser window.

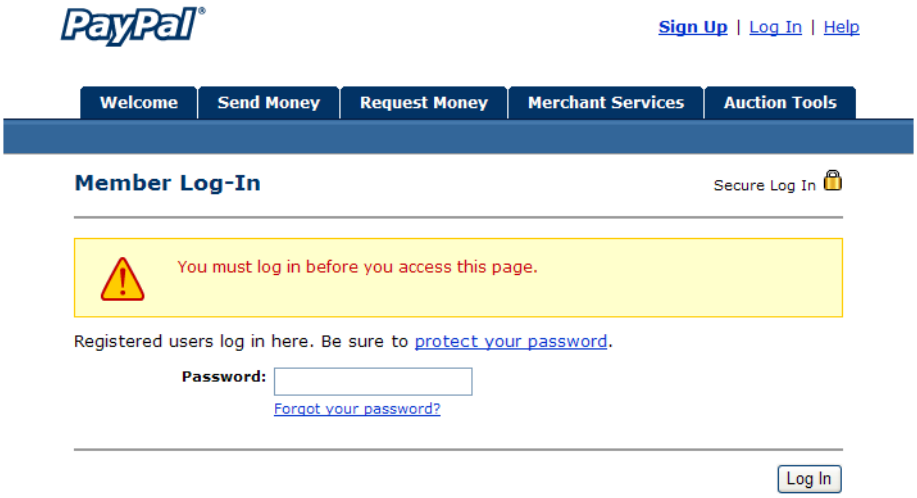

Fig. 3. The content of a real, but confusing, PayPal page. Many participants found this page suspicious because it does not ask for a username. The group trained about extended validation was more likely to correctly label this page as legitimate.

- **Real, but confusing, site.** A deep link into a real site shown in the familiarization step. The page features a warning screen and asks the user for their password, but not a username, as shown in Fig. 3. PayPal regularly sends emails linking to such pages.
- **Homograph attack.** A phishing web page with a domain name that is only a few pixels different from the legitimate site's domain name. The attack sites were `www.bankofthevvest.com` and `www-bankofthewest.com`.
- **Homograph with suspicious page warning.** A homograph attack that triggers a yellow suspicious page warning in Internet Explorer 7. The attack sites were `www.paypai.com` and `www.paypa1.com` (the l is the numeral `1`).
- **Picture-in-picture attack.** A phishing web page that shows a fake browser window that appears to be showing the real site.
- **Mismatched picture-in-picture attack.** A picture-in-picture attack that shows a fake browser with a different color scheme than the color scheme of the operating system.
- **IP address blocked by phishing filter.** A web site with no domain name (only a numerical IP address). The browser was immediately navigated away from the page by the Internet Explorer phishing filter, and the address bar turned red. Phishing sites often use IP addresses rather than domain names, but in certain security schemes IP addresses can also be used by legitimate banking sites [28].

3.3 Implementation

During the tasks, the participants used a Windows XP desktop machine in a quiet lab setting. The machine was configured using a `hosts` file containing modified DNS entries for both the spoof and the legitimate domains used in the study pointing to our lab web servers. Additionally, the browser's certificate database had been augmented with our own self-signed root certificates, enabling us to forge regular and extended validation certificates. Our lab servers were thus able to mount a "man-in-the-middle" attack, intervening between the participant's computer and the real site. The lab web servers acted as reverse proxies, contacting the "real" web site over the Internet on every request and forwarding the response back to the participant's computer with minor changes, simulating the experience of extended validation certificates on the real sites. This configuration also enabled us to construct convincing phishing sites that were exact copies of the real site, differing only in the domain name.

To simulate picture-in-picture attacks, we developed a fake implementation of Internet Explorer in JavaScript, simulating many of the features that a user might use when determining whether a site is legitimate. The simulated browser provided a realistic-looking address bar and a lock icon that displayed fake certificate details when clicked. We provided a fake phishing filter that reported the site as "not a suspicious or reported phishing web site." The fake browser could be navigated, closed, and even dragged, although it could not be dragged outside the confines of the parent page.

3.4 Participant Recruitment and Demographics

Our 27 participants were recruited through the Microsoft Research Usability recruiting service. Two of the participants were non-technical Microsoft employees, and the rest were living in the greater Seattle area, but not affiliated with Microsoft. Potential participants were invited to participate in a study involving "usability of online banking," but were not told ahead of time that the study involved security. For participating, participants received their choice from a list of Microsoft software products.

The participants were 59% male (16) and 41% female (11). None of them were colorblind, and all used Windows as their primary operating system with Internet Explorer as their primary browser. Of the two sites used in the study, none of them had heard of Bank of the West before, whereas 59% (16) had used PayPal. Most, 82% (22), had some experience with online financial services. The average hours of computer usage per week was 36 (min 6, max 80, s.d. 17). Of the participants, 7 (26%) held Masters degrees, 9 (33%) held Bachelors degrees, 9 (33%) reported attending some college, and two held high school diplomas. The average age was 47 (min 23, max 55, s.d. 7.6).

After the tasks, but before the debrief, we asked the participants a few questions to assess their awareness of browser encryption. When shown a picture of an unsecured wireless connection dialog, 88% (23 of 26 respondents) thought that they would be vulnerable to electronic eavesdropping while using the connection

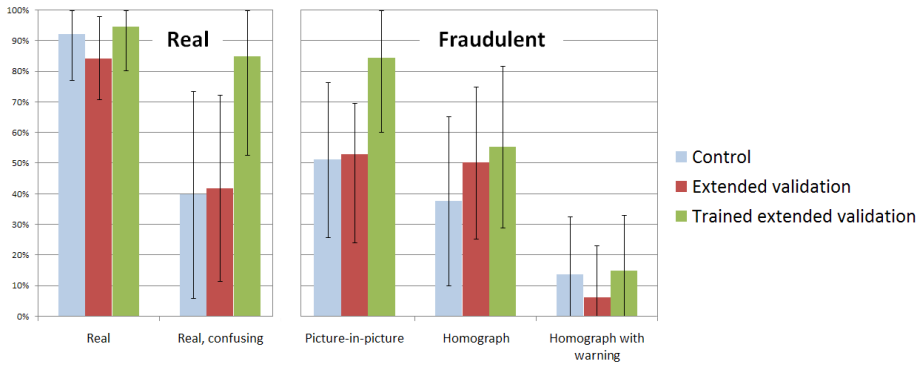

Fig. 4. Percentage of participants who classified sites as legitimate. (95% confidence)

for bank transactions, as well as while using the connection to read emails from a web email account. The other 12% (3) thought that they would be secure against electronic eavesdropping while using both types of sites. Because none of the participants provided a different response based on the type of site visited (bank sites use HTTPS, whereas web email sites generally use plain HTTP after the login page), these observations suggest that the participants were not browser encryption experts.

4 Results

A summary of the data collected appears in Fig. 4. Trained participants were more likely to classify the real, confusing site as legitimate, both compared with untrained (p=.031) and with control users (p=.032). The picture-in-picture attacks were more likely to succeed against trained participants than against those in the control group (p=.042), but the observed difference with the untrained group is marginally insignificant (p=.051). Other observed differences in classification were insignificant.

One of the picture-in-picture attacks had silver chrome that matched the operating system theme and two had blue chrome that did not match. Across all groups, we did not observe a significant effect of the chrome color on classification (Friedman's Chi-Square = 0.77, df=1, p=.782). The matched and mismatched picture-in-picture attacks were both classified legitimate by the same percentage of participants (63%).

Across all groups, we did not observe a significant effect of participants having a PayPal account on accurately classifying sites (F=1.12, p=.301) or, specifically, on accurately classifying PayPal sites (F=1.82, p=.191). Because none of the participants had heard of Bank of the West before, we were unable to measure the effect of having an account at Bank of the West on classification choices.

Only three participants categorized all three of the picture-in-picture attacks as fraudulent. Two of these participants tried to use browser features that were not implemented in our JavaScript browser simulation (right clicking and advanced certificate dialog features) and labeled the site as fraudulent because they were not able to get the feature to work. The other participant refused to label any popup window as legitimate.

Across all groups, participants were fooled by homograph pages 11% of the time if a "suspicious page" warning was displayed, compared to 48% of the time if no warning was displayed ($t(26)=4.48$, $p<.001$). Although the effect of the warnings is statistically significant, its applicability is limited because the participants were aware that they needed to classify sites (see discussion in Section 5.5). We also included an IP address that was on the phishing blacklist, which none of the participants classified as legitimate.

When asked afterwards which browser features they had used to categorize web sites as legitimate or fraudulent, 4 of the trained participants indicated that they had used the browser address bar color, one participant in the control group noticed the yellow and red warning colors, and no users in the experimental group indicated that they had used any of the colors.

5 Discussion

5.1 Evaluating extended validation

We did not find that extended validation provided a significant advantage in identifying the phishing attacks tested in this study. The untrained extended validation group performed similarly to the control group on all tasks, and none of the untrained extended validation group participants indicated that they had used the address bar color in classifying sites. Extended validation could become more effective over time as it is adopted by more financial web sites and public awareness grows, but at the time of our study (September 2006) we did not observe that it had a significant effect on user behavior.

5.2 Documentation

The trained group was more likely to classify both real and spoof sites as legitimate. This effect can be explained because the portion of the Internet Explorer 7 help files used as the training document included a description of extended validation as well as phishing warnings. Several participants in the trained group focused on the phishing warnings description, expecting that every phishing page would show a warning. This expectation caused them to ignore the lack of an extended validation indicator at some homograph and picture-in-picture pages, and it helped them accurately classify the real (but confusing) sites as legitimate. These findings suggest that browser documentation should be carefully designed not to give the impression that the phishing filter is 100% accurate. In order to isolate the effect of training on extended validation, we plan to limit the training to extended validation for a subsequent study in this area.

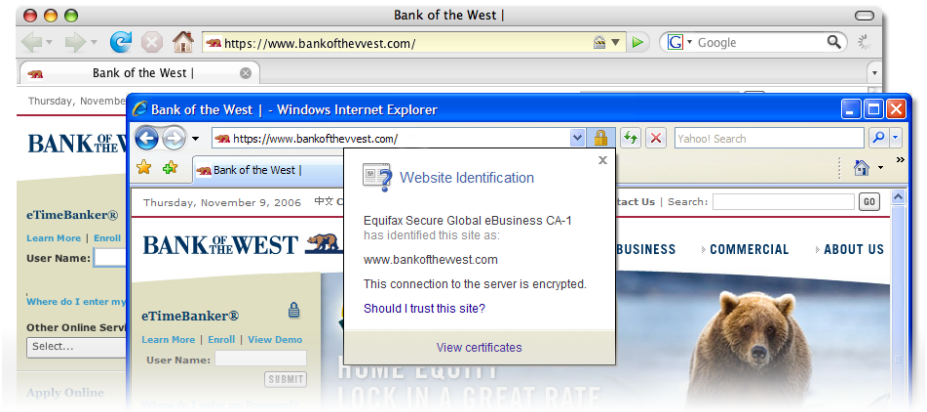

Fig. 5. Comparison of homograph attack on MacOS X with Firefox 2 and Windows XP with Internet Explorer 7

5.3 Homograph defenses

Across all groups, the spoof rate for the "bankofthevvest" homograph attack on Internet Explorer 7 with a Windows XP PC was lower than than the 91% observed by Dhamija et. al. [12] using Firefox on a MacOS X laptop. The font used in the address bar for Mac Firefox has no gap between the double "v" characters, rendering the homograph attack very effective. Internet Explorer 7 on Windows XP has a gap between "v" letters in the address bar, making the attack easier for users to detect. The certificate details popup, however, uses a font with no gap. One user who looked at the certificate details but not the address bar was fooled by the homograph attack. A comparison of the fonts is shown in Fig. 5.

One proposed defense against homograph attacks is to detect visually deceptive domain names using automated algorithms [29]. It is particularly important to provide this protection in the presence of international Unicode characters, which are hard to distinguish with the naked eye. Internet Explorer 7 disables rendering of international domain names that are not part of the user's configured language.

5.4 Picture-in-picture defenses

The general problem of protecting users from spoofed user interfaces in an overlapping window environment is difficult. Although complete solutions do exist [18], they require user interface changes that might seem unnecessary to the user. Without changing the current browser user interface, there are still some visual cues that can be used to identify these attacks.

- **Popups.** External links that open in a new window disable the Back button and can often be perceived as an annoyance [30], yet these links still appear on many major web sites, such as Google's Gmail. Recently, browsers have been discouraging new windows with popup blockers, and browsers such as Firefox and Opera open links in new tabs instead of new windows, when possible. When users restrict their browsing to a single window, the address bar is a more reliable indicator of identity.
- **Mismatched chrome.** One way to expose fake browser windows is to make real browser windows customized for each user, requiring the attacker to guess wildly in order to make a convincing fake [19]. In our study, we observed no significant difference in response when the inner (fake) window had a different chrome color than the outer (real) windows, but the participants were not told to pay attention to the chrome color. This scheme might work better with training. However, most participants found it difficult to notice that the inner window was the wrong color, even during the debrief when it was pointed out to them. Theme differences in Windows applications, such as the Mac-like iTunes interface and the Nullsoft Winamp media player, might have desensitized users to mismatched chrome. Populating the address bar area with a custom icon [25] could be a more effective solution than custom themes.
- **Focus.** In the Windows XP operating system, only one window can be focused at a time. Only the focused window has a bright ("active") title bar. The outer attack page must be focused for the user to enter information into the fake inner window. Thus, a user who sees two focused windows (or a browser window that is focused but appears inactive) can conclude that a fake browser window is present. Unfortunately, this distinction is subtle and hard to remember.
- **Dragging.** A fake browser window cannot be dragged outside of its parent window. Attempting to drag a browser window outside of its parent can thus be used to identify picture-in-picture attacks. However, merely dragging the window around inside its parent does not provide any information about the authenticity of the window.
- **Maximizing.** A fake browser window cannot be maximized, so maximizing a window is an easy way to know that a browser window is not fake. However, windows that cannot be maximized are not a sure sign of fraud as some legitimate sites create popup windows that cannot be maximized.

5.5 Phishing filter

Some test pages triggered phishing warnings. Those participants who labeled pages with a phishing warning as legitimate did so because they did not notice the warning. However, not all of the fraudulent sites triggered phishing warnings, simulating the reality that phishing warnings appear at some, but not all, phishing sites. By including these warnings, we account for the false sense of security provided by the warnings that might cause users to ignore the extended validation indicator. Our scenario was designed to test the participants' understanding

of the browser security indicators, not their awareness of the possibility of an attack. Thus, we explicitly instructed participants to look for fraudulent pages. A study scenario that includes tasks unrelated to security, such as [16], can be used to measure the absolute effectiveness of phishing warnings in real-world scenarios; our results only provide an upper bound on effectiveness.

6 Conclusion

New browser technologies such as extended validation have the potential to defend against fraud by identifying the source of the content displayed on the screen. In this paper, we presented a controlled between-subjects evaluation of the extended validation user interface in Internet Explorer 7. Unfortunately, participants who received no training in browser security features did not notice the extended validation indicator and did not outperform the control group. The participants who were asked to read the Internet Explorer help file were more likely to classify both real and fake sites as legitimate whenever the phishing warning did not appear.

If extended validation becomes widespread, we expect that online criminals will try to mimic its trust indicator, just as they have copied other legitimate financial websites in the past. Like its predecessor, the lock icon, extended validation is vulnerable to picture-in-picture user interface spoofing attacks. We found these attacks to be as effective as homograph attacks, the best known phishing attack. Designing a user interface that resists both homograph and picture-in-picture attacks should be a high priority for designers of future browsers.

References

1. Felten, E.W., Balfanz, D., Dean, D., Wallach, D.S.: Web Spoofing: An Internet Con Game. In: 20th National Information Systems Security Conference. (October 1997)
2. Anti-phishing working group: `http://www.antiphishing.org`
3. Loftesness, S.: Responding to "Phishing" Attacks" (2004) `http://www.glenbrook.com/opinions/phishing.htm`.
4. Franco, R.: Better Website Identification and Extended Validation Certificates in IE and Other Browsers (November 2005) IEBlog.
5. Gabrilovich, E., Gontmakher, A.: The Homograph Attack. Communications of the ACM **45**(2) (2002)
6. Chou, N., Ledesma, R., Teraguchi, Y., Mitchell, J.: Client-side defense against web-based identity theft. In: Proceedings of Network and Distributed Systems Security (NDSS). (2004)
7. Google, Inc.: Google safe browsing for firefox Accessed: November 1, 2006. `http://www.google.com/tools/firefox/safebrowsing/`.
8. Netcraft: Netcraft Anti-Phishing Toolbar Accessed: November 1, 2006. `http://toolbar.netcraft.com/`.
9. GeoTrust, Inc.: TrustWatch Toolbar Accessed: November 1, 2006. `http://toolbar.trustwatch.com/`.

10. Zhang, Y., Egelman, S., Cranor, L., Hong, J.: Phinding Phish: Evaluating Anti-Phishing Tools. In: Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS). (2007)
11. Whalen, T., Inkpen, K.M.: Gathering evidence: use of visual security cues in web browsers. In: GI '05: Proceedings of the 2005 conference on Graphics interface, School of Computer Science, University of Waterloo, Waterloo, Ontario, Canada, Canadian Human-Computer Communications Society (2005) 137–144
12. Dhamija, R., Tygar, J., Hearst, M.: Why Phishing Works. In: Proc. CHI. (2006)
13. Netcraft: Cardholders targetted by Phishing attack using visa-secure.com (October 2004) `http://news.netcraft.com/`.
14. Inc., V.: VeriSign Certification Practice Statement (November 2006) `http://www.verisign.com/repository/CPS/VeriSignCPSv3.3.pdf`.
15. Whitten, A., Tygar, J.: Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In: 8th Usenix Security Symposium. (1999) 169–184
16. Wu, M., Miller, R., Garfinkel, S.: Do Security Toolbars Actually Prevent Phishing Attacks? In: Proc. CHI. (2006)
17. Passmark: `http://www.passmarksecurity.com`
18. Ye, Z.E., Smith, S., Anthony, D.: Trusted Paths for Browsers. ACM Transactions on Information and System Security **8**(2) (2005) 153–186
19. Dhamija, R., Tygar, J.: The Battle Against Phishing: Dynamic Security Skins. In: SOUPS '05: Proceedings of the Symposium on Usable Privacy and Security. (2005)
20. Dierks, T., Allen, C.: The TLS Protocol — Version 1.0. IETF RFC 2246 (January 1999)
21. Parno, B., Kuo, C., Perrig, A.: Authentication and Fraud Detection: Phoolproof phishing prevention . In: Proceedings of Financial Cryptography and Data Security (FC '06). (2006)
22. Chappell, D.: Introducing Windows CardSpace (2006) `http://msdn2.microsoft.com/en-us/library/aa480189.aspx`.
23. Halderman, J.A., Waters, B., Felten, E.: A convenient method for securely managing passwords. Proceedings of the 14th International World Wide Web Conference (WWW 2005) (2005)
24. Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J.: Stronger Password Authentication Using Browser Extensions. In: Proceedings of the 14th Usenix Security Symposium. (2005)
25. Yee, K., Sitaker, K.: Passpet: convenient password management and phishing protection. In: SOUPS '06: Proceedings of the second symposium on Usable privacy and security, New York, NY, USA, ACM Press (2006) 32–43
26. Wu, M., Miller, R.C., Little, G.: Web Wallet: Preventing Phishing Attacks by Revealing User Intentions. In: SOUPS '06: Proceedings of the Symposium on Usable Privacy and Security. (2006)
27. Chiasson, S., van Oorschot, P., Biddle, R.: A Usability Study and Critique of Two Password Managers. In: Proc. 15th USENIX Security Symposium. (2006)
28. Juels, A., Jakobsson, M., Stamm, S.: Active Cookies for Browser Authentication. In: Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS). (2007)
29. Fu, A.Y., Deng, X., Wenyin, L., Little, G.: The methodology and an application to fight against unicode attacks. In: SOUPS '06: Proceedings of the second symposium on Usable privacy and security, New York, NY, USA, ACM Press (2006) 91–101
30. Nielsen, J.: The top ten web design mistakes of 1999 (May 1999) `http://www.useit.com/alertbox/990530.html`.