Failure to Recognize Fake Internet Popup Warning Messages

David Sharek, Cameron Swofford, and Michael Wogalter
Psychology Department, North Carolina State University
Raleigh, NC 27695-7650 USA

"Warning, your computer is infected with spyware. Windows needs to download and install the anti-spyware updates to remedy this issue. Click OK to begin." This is just one example of many popup warnings that spyware and malware creators use to try to mislead unsuspecting Internet users into downloading potentially harmful software. Falling prey to an illegitimate message could produce negative consequences that vary from bothersome computer performance to complete system failure. The purpose of this study was to determine which visual design cues, if any, would alert people to the illegitimacy of fake popup warning windows while browsing the Internet. Results indicated that most people did not behave in a cautious manner upon presentation of three different fake popup warning windows. Implications of the research are discussed.

INTRODUCTION

Determining the credibility of popup warning windows or dialog boxes can be difficult because of the broad range of Internet technologies that can mimic real local operating system messages. Individuals may believe that an error message originates from a legitimate source such as their personal computer's operating system when the warnings are actually illegitimate Internet popup messages. Some of the technologies available to produce realistic but phony windows include Cascading Style Sheets, Layers and Adobe Flash. These and other applications can be used to mimic legitimate operating system errors. Fortunately, there are several cues that can assist Internet users in making an accurate discrimination between real and fake operating system messages. Unfortunately, many Internet users may not be aware of these distinctions.

Recognition of a website's credibility is frequently left to the individual Internet user to discern (Flanagin & Metzger, 2007; Wogalter & Mayhorn, 2008). In those situations users may rely on specific cues to determine credibility including features that reflect expertise, a professional look and feel, and a positive assessment of the website owner's photograph (Eysenbach & Kohler, 2006). These elements can easily be manipulated to give the impression of authenticity (Evil, Shaver, & Wogalter, 2003; Freeman & Spyridakis, 2004).

Dhamija, Tygar, and Hearst (2006) noted that "some visual deception attacks can fool even the most sophisticated users." Even after participants were told to expect some websites to be false, 90% of the participants were still fooled by phony websites. Dhamija et al. (2006) report that people lack knowledge about characteristics on how some webpage and browser elements behave. For example, many did not know that the cursor icon does not change when held over elements in a legitimate system error message. Also, they were not aware of other aspects of web browser interfaces such as the tool and address bars. Dhamija et al. (2006) report that 23% of their participants used only portions of a page's content, such as its logo, layout, and graphic design to determine website credibility.

The present study focused on several design elements that can be used to produce illegitimate warning windows. The illegitimate windows were of the type that might be used by adware and malware creators to trick unsuspecting Internet users into clicking on them, thus opening their computers to attack. The severity of these negative consequences ranges from bothersome irregularities, such as slow performance, to complete system failure. Innocent-appearing clicks on OK buttons could lead to the downloading of potentially nefarious programs that can gather personal information which can compromise privacy and lead to more serious problems such as identity theft.

The present research sought to determine if people would behave more cautiously when presented with fake popup warning windows while performing an online browsing task.

Response time, and the choice of button that participants chose to click on, with respect **to both real and fake popup warning windows, was recorded.** Also collected in a post-task questionnaire were reports of prior knowledge of fake popup warnings and the reasons why participants clicked on the button they chose.

METHOD

A total of 42 university undergraduates participated (23 males, 21 females; mean age = 19 years, SD = 4.5).

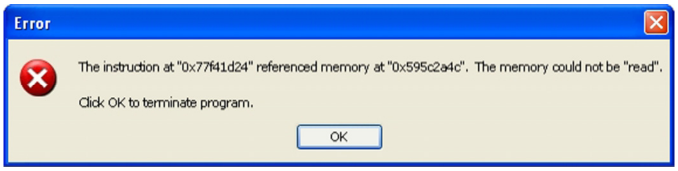
The apparatus for this experiment included a computer running Windows XP Service Pack 2, a MySQL database used to collect participant responses, and a specially designed Internet browser simulator. The 17 inch (43.2 cm) LCD monitors provided a resolution of 1024 x 768.

In order to maintain visual consistency, the websites were pre-designed to remain unchanged from the first to the last participant. Participants were told that all links were disabled to prevent them from viewing other pages. In order to create or enhance the impression of actually browsing the Internet, the participants were led to believe that the websites were downloaded from the Internet in real-time. While viewing the websites, participants experienced events in which popup warning windows were displayed. Data on how the participants responded to these warnings (what buttons they clicked on) as well as their response times were collected. After viewing all of the websites, the participants answered a follow-up questionnaire and were then debriefed and thanked for their time.

In order to create a completely controlled viewing environment, Adobe Flash CS3, running at 32 frames-per-second to simulate Microsoft's Internet Explorer (version 7.0.5730.11) was used. Twenty different health websites were programmed to load in a similar way as real websites. For example, larger images loaded slower, text appeared before animations, the cursor updated when hovering over website links and browser elements, the correct time and date was always visible, and the status bar indicator updated during download. Health websites were used because they are generally perceived to be credible (Metzger, 2007). Other sites such as news sites were also considered, but the time-sensitive nature of the content would have made it difficult to maintain updates. In post experiment interviews, several participants reported amazement that they did not view a real browser, and one even indicated annoyance with the website load time.

The popup windows were designed to follow the standard presentation of error messages in Microsoft Windows XP. The text was also similarly designed. The message displayed was "*The instruction at '0x77f41d24' referenced memory at '0x595c2a4c.' The memory could not be 'read.' Click OK to terminate program.*" The four popup variations used are shown in Figures 1 to 4. **Figure 1** illustrates a legitimate (real) warning error message. It looked and acted exactly like a real system error. Figures 2 to 4 illustrate illegitimate (fake) popup warning windows. They contained non-standard visual elements.

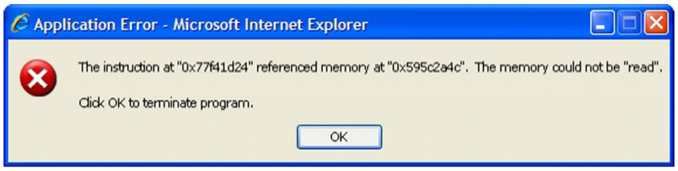
Figure 1. Real popup warning window



The instruction at "0x77f41d24" referenced memory at "0x595c2a4c". The memory could not be "read".

Click OK to terminate program.

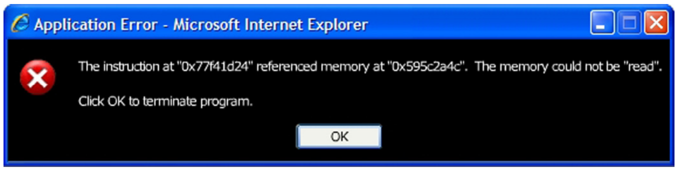
Figure 2. Fake popup warning window (Fake 1)



The instruction at "0x77f41d24" referenced memory at "0x595c2a4c". The memory could not be "read".

Click OK to terminate program.

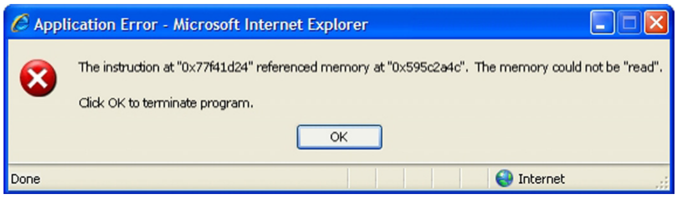
Figure 3. Fake, flashing popup warning window with black background visible (Fake 2)



The instruction at "0x77f41d24" referenced memory at "0x595c2a4c". The memory could not be "read".

Click OK to terminate program.

Figure 4. Fake popup warning window with minimize button and status bar (Fake 3)



The instruction at "0x77f41d24" referenced memory at "0x595c2a4c". The memory could not be "read".

Click OK to terminate program.

One variation of the fake warning message, shown in **Figure 2**, was designed from a single, clickable image that, on mouse hover, changes the cursor to a hand icon. The minimize button was also visible.

A second variation of a the fake warning message, shown in **Figure 3**, used the same design elements as shown in Figure 2 with the addition of a flashing background (inverse black to white). This flashing technique is commonly used in electronic displays to attract attention.

The third fake warning message, shown in **Figure 4**, included (a) the minimize button at the top-right of the popup window, (b) the Internet browser's status bar located at the bottom, and (c) when the cursor hovered over the 'OK' button, it changed to the hand icon. All of these differences are created by, and indicative of, a webpage opening a new browser window, centering it in the middle of the screen, and disabling resizing controls.

Each participant was randomly assigned a number which they entered into the program in order to begin participation. Each participant viewed 20 websites each for 30 seconds. After each website presentation, participants rated the last-viewed website on the extent of clutter on the page on a 9-point scale using an online form. The rating task was intended to disguise the true reason for the study and to keep participants interested in the material shown on the screen

The 4 popup error message windows appeared approximately 5 seconds into viewing every 5th website. Participants were exposed to all 4 popup warning variations. The order in which the popup windows were presented was balanced using a Latin square.

Data were collected on both how long it took participants to click on the first warning window that they were presented with, and which buttons they clicked on, including if they did not click on anything and just left the window alone, or dragged it off screen.

Clicking on the popup's close button (indicated by an 'X' at the top right of the window) was considered to be the correct way of dealing with fake popup warning windows. Clicking on the minimize button, the window as a whole, or the OK button was considered to be an indication that the participant was fooled by the window and did not recognize that it was fake.

After viewing the websites, the participants were shown the first popup they saw with highlights around the areas that they clicked on. They were asked why they clicked on those areas. Other questions asked about their knowledge of fake popup warning windows. After completing the above procedure, participants were debriefed and thanked.

RESULTS

Two main analyses were performed on the data. The first considers only how the participants reacted to the first error message they had seen. Because of strict assignment to the counterbalancing (Latin Square) scheme, a smaller but equal number of participants were available in each cell (cell size, $n = 10$); this avoided carry-over effects. A second analysis considers responses to all four of the error messages, regardless of the order that the participants viewed them in.

The first analysis revealed that the close button was selected 29% of the time, the OK button was selected 63% of the time and 7% of the participants simply dragged the window out of their way and continued viewing the websites. No one minimized the window.

Response time (M = 13.74 seconds, SD = 14.74 seconds) for the first popup window viewed was not significantly different between any of the four conditions, $F(3, 34) = 1.16$, $p = .34$, $\eta^2 = .09$.

Previous knowledge of fake popup warning windows was not significantly associated with the likelihood that a participant would click on the close button, $\Phi = .22$, $p = .16$, $\Phi^2 = .05$. Previous knowledge accounted for 5% of variability in the likelihood of clicking on the correct button.

Data from the post task questionnaire indicated that 12% of those who clicked on the OK button indicated that they did so because the text told them to, while 23% said they always click on that button when they encounter error messages. Just under half (42%) responded that they just wanted to "get rid of it." Six individuals (23%) chose to phrase their own answers. Three of the six indicated that they did not see any other choice that they could make.

Table 1. Frequencies of which buttons were clicked for each of the 4 popup warning windows

	Warning Windows			
Buttons	Real	Fake 1	Fake 2	Fake 3
Close (X)	11	11	9	12
OK	26	25	25	23
Minimize	2	3	4	4
Drag	1	1	2	1

As can be seen in **Table 1**, the second analyses revealed that the majority of participants clicked on the OK button regardless of whether the warning was legitimate or not. The OK button was clicked 62% of the time and the close button was clicked 27% of the time.

Table 2. Frequencies (and percentages) of correct and incorrect participant responses for the real warning and fake popup warning windows

Response	Real Warning	Fake Warning Windows
Correct	26 (65)	32 (27)
Incorrect	14 (35)	88 (73)

As can be seen in **Table 2,** the majority of participants responded correctly to the real warning window and incorrectly to the fake warning windows. The correct response to the real warning window was to click the OK button and the correct response to the fake warning windows was to click the close button. Seventy three percent of the participants incorrectly responded to the fake popup warning windows by not clicking on the close button. A Chi-square showed that there was a significant effect of real vs. fake warnings on responses, X^2 (1, N = 40) = 19.08, p < .01.

DISCUSSION

The present study examined some of the methods used by adware and malware creators to trick unsuspecting Internet users into clicking on buttons that could open them up for attack by malicious software. Realistic-appearing, but fake error messages were presented while participants performed a task of looking at, and rating a set of 20 web pages on clutter. Findings revealed that many people responded in ways that indicated that they did not realize the potential negative consequences that could result if they clicked the OK button instead of the close button when presented with a fake popup warning window.

When faced with both real and fake popup warning windows, the majority of participants selected the OK button. In regards to the fake warning windows, this was the riskiest option. Clicking on this button, or any button other than the close button, could potentially redirect the participant to a website where spyware and other harmful malware could be downloaded. This behavior implies that many people fall for this style of attack by not recognizing the visual elements that separate real and fake warning windows.

Responses from the post-task questionnaire indicate that annoyance with the messages may have contributed to unsafe clicking behavior. Nearly half of the participants (42%) reported that they just wanted to “get rid of” the error message. Participant responses suggest that they simply did not want to deal with error messages.

The study indicates that false error messages could pose problems if their appearance is very near to that of real operating system error messages. The results suggest a lack of knowledge by users in the characteristics (design inconsistencies) that distinguish real and fake error messages, and that users seem to have little awareness of the potential risks involved in clicking on fake popups. Making prominent unique features of real error messages and educating users may be useful ways to decrease the problems noted in this research, and are potential topics for future research.

Additional work might also examine how people react in a similar study carried out with greater involvement of personal risk such as displaying the error messages on the participants’ personal computers.

REFERENCES

Dhamija, R., Tygar, J.D., & Hearst, M. (2006). Why phishing works. *CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems,* 581-590.

Evil, A. Y., Shaver, E. F., & Wogalter, M. S. (2003). On trust in the Internet: Belief cues from domain suffixes and seals of approval. *Proceedings of the Human Factors and Ergonomics Society*, 47, 1346-1350.

Eysenbach, G., & Kohler, C. (2002). How do consumers search for and appraise health information on the world wide web? Qualitative study using focus groups, usability tests, and in-depth interviews. *British Medical Journal*, 324, 573-577.

Flanagin, A. J., & Metzger, M. J. (2007). The role of site features, user attributes, and information verification behaviors on the perceived credibility of web-based information. *New Media Society*, 9, 319-342.

Freeman, K. S., & Spyridakis, J. H. (2004). An Examination of Factors That Affect the Credibility of Online Health Information. *Technical Communication*, 51, 239-263.

Metzger, M. J. (2007). Making sense of credibility on the Web: Models for evaluating online information and recommendations for future research. *Journal of the American Society for Information Science and Technology*, 58, 2078-2091.

Wogalter, M. S., & Mayhorn, C. B. (2008). Trusting the Internet: Cues affecting perceived credibility. *International Journal of Technology and Human Interaction*, *4*, 76-94