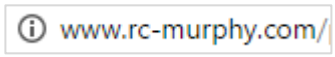
Perceptions of Online Security Indicators

Robert Murphy, Symantec, 2015

Background

When collecting personal information, website developers should use SSL certificates on their webservers to assure the collected data is encrypted and secured. When SSL is implemented, browsers display security indicators as part of the URL and web pages can display the branded security seal as an additional indicator of the security of the page.



Problem

It wasn't clear how effective the security indicators are: how much trust do they afford to the user and what affect do they have on the users' behavior? Numerous studies have been conducted, but each with their limitations, such as being biased with the context of security; being limited in scope of research; and being performed in a lab setting, which was perceived as 'secure'.

Solution

I developed a methodology that measures user's likelihood to continue their on-line activity in different scenarios where personal information is collected. Participants were shown screen shots of web pages that ask for information such as user-name and password, social security number, or credit card / payment data.

Implementation

The context of the study was an evaluation of web pages, so the concept of security was absent until follow up questions. Various implementations of browser security indicators and seals were used in the display of fictitious web pages. Quantitative feedback was collect from *likelihood of continuing* scale responses and qualitative feedback was collected through explanation of *why* they chose the particular response.

Analysis

We were able to learn what percentage of users rely on security indicators when submitting personal information, what browser security indicators and security seal brands are most effective, and what colors and verbiage are the most effective in security seal designs.