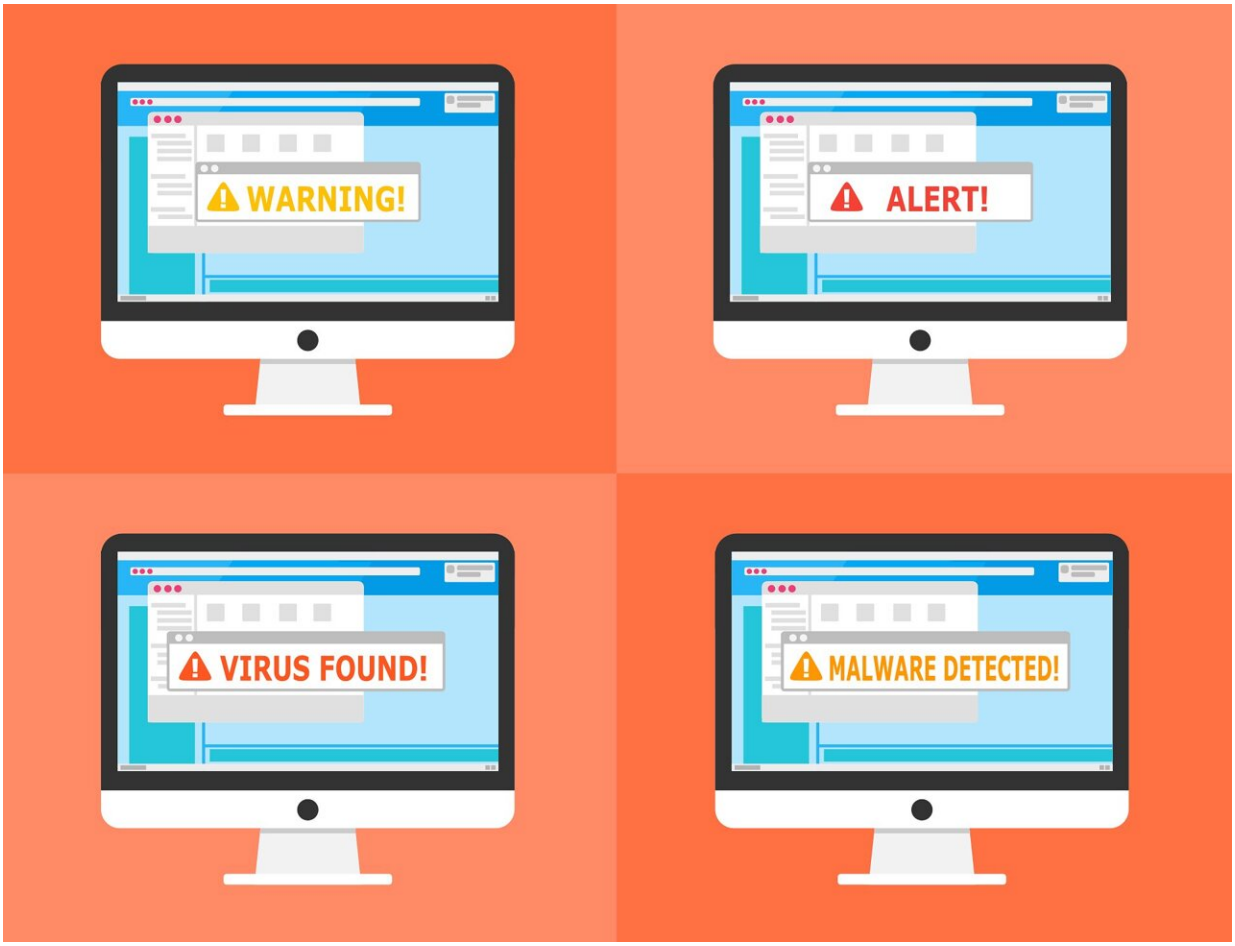
Interactive security prompts help promote more secure behavior online, finds study

January 27 2023, by Shea Walters



Credit: Pixabay/CC0 Public Domain

You're busy working on a project when suddenly a security message

appears on your screen, warning of a potential security risk. Do you act, or do you ignore and quickly return to work? If the message includes a list of security dos and don'ts, then you are likely to ignore it if you are like most people.

Persuasive security messages, known as fear appeals, are used to warn users of security vulnerabilities and prompt behavior change. Often ignored, they can come in the form of online password prompts—such as password strength meters and password improvement suggestions.

However, if the fear appeal is interactive and provides real-time feedback in response to the user's actions, the user is more likely to engage with the message while online, according to research from Virginia Tech Pamplin College of Business faculty Anthony Vance.

In a study published in *MIS Quarterly*, Vance, professor and Commonwealth Cyber Initiative Fellow in the Department of Business Information Technology and director of Pamplin Integrated Security, and his co-authors, tested the effectiveness of interactive fear appeals that would interrupt users during tasks such as browsing the internet, studying, online shopping, and more. He explored how interactive fear appeals can encourage people to act more securely while conducting other online tasks.

To test the theory that interactive fear appeals can encourage more secure behavior, researchers partnered with Socwall.com, a repository for computer wallpaper images with an average of 10,000 daily users, to test different types of fear appeals on participants while they created passwords on the site.

The experiment took place over a one-month period with 427 consenting users who were browsing wallpapers on the site. The researchers developed an interactive tool that measured and communicated password

strength in terms of the estimated time it would take for an attacker to crack the password and shared this information in real time as users adjusted their passwords.

They tested four treatments: the control with no password feedback to the user, an interactive-only treatment with a traditional password strength meter without improvement suggestions, a non-interactive fear appeal with a detailed list of guidelines and a short warning, and an interactive fear appeal with a warning message and the dynamic "time to crack" password prompt.

When participants visited the registration page of Socwall.com, the web server randomly assigned one of the four treatments, requiring them to create a unique username and password for their accounts.

The research demonstrated how interactive fear appeals led to passwords that were 39 times stronger than passwords created by users with non-interactive fear appeals. Contrary to conventional wisdom, the password strength meter treatment did not result in stronger passwords.

To deepen their understanding of these outcomes, the researchers conducted focus groups with 40 student participants to uncover additional feedback on each of the appeals.

Affirming the results of the field study, the majority of participants agreed that the real-time feedback provided in the interactive fear appeal was the strongest motivator to take action to improve their password security.

When the students reviewed the password strength meter treatment, they had difficulty putting the meter into context. For the non-interactive fear appeal, students struggled to sift through the large quantity of information included in the guidelines and discern whether their new

password was strong.

The research demonstrated how interactive fear appeals are more compelling than the other types of treatments tested in the study. By making fear appeals more interactive, it spurs greater cognitive engagement in the task by users and encourages them to follow through on the request and practice more secure behavior while conducting online activities for work, school, and more.

Finding ways to make fear appeals more engaging is especially important when a fear appeal interrupts a person's work.

"When fear appeals are delivered as a secondary task they interrupt the user's work (i.e., the primary task), like responding to email. This typically results in the user ignoring the fear appeal which leaves the user or their organization vulnerable to cyber threats," said Vance.

The results have implications for fear appeals in cybersecurity contexts beyond password security.

"It is easy to see how these findings can be applied to fear appeals around threats of malware, phishing, or even in contexts such as privacy settings or firewall configurations, which if mishandled, can lead to dangerous outcomes concerning a person's security and privacy," said Vance.

More information: Anthony Vance et al, Do Security Fear Appeals Work When They Interrupt Tasks? A Multi-Method Examination of Password Strength, *MIS Quarterly* (2022). DOI: 10.25300/MISQ/2022/15511

Provided by Virginia Tech