

Effective Notification Campaigns on the Web: A Matter of Trust, Framing, and Support

Abstract:

Misconfigurations and outdated software are a major cause of compromised websites and data leaks. Past research has proposed and evaluated sending automated security notifications to the operators of misconfigured websites, but encountered issues with reachability, mistrust, and a perceived lack of importance. In this paper, we seek to understand the determinants of effective notifications. We identify a data protection misconfiguration that affects 12.7% of the 1.3 million websites we scanned and opens them up to legal liability. Using a subset of 4754 websites, we conduct a multivariate randomized controlled notification experiment, evaluating contact medium, sender, and framing of the message. We also include a link to a public web-based self-service tool that is run by us in disguise and conduct an anonymous survey of the notified website owners (N=477) to understand their perspective.