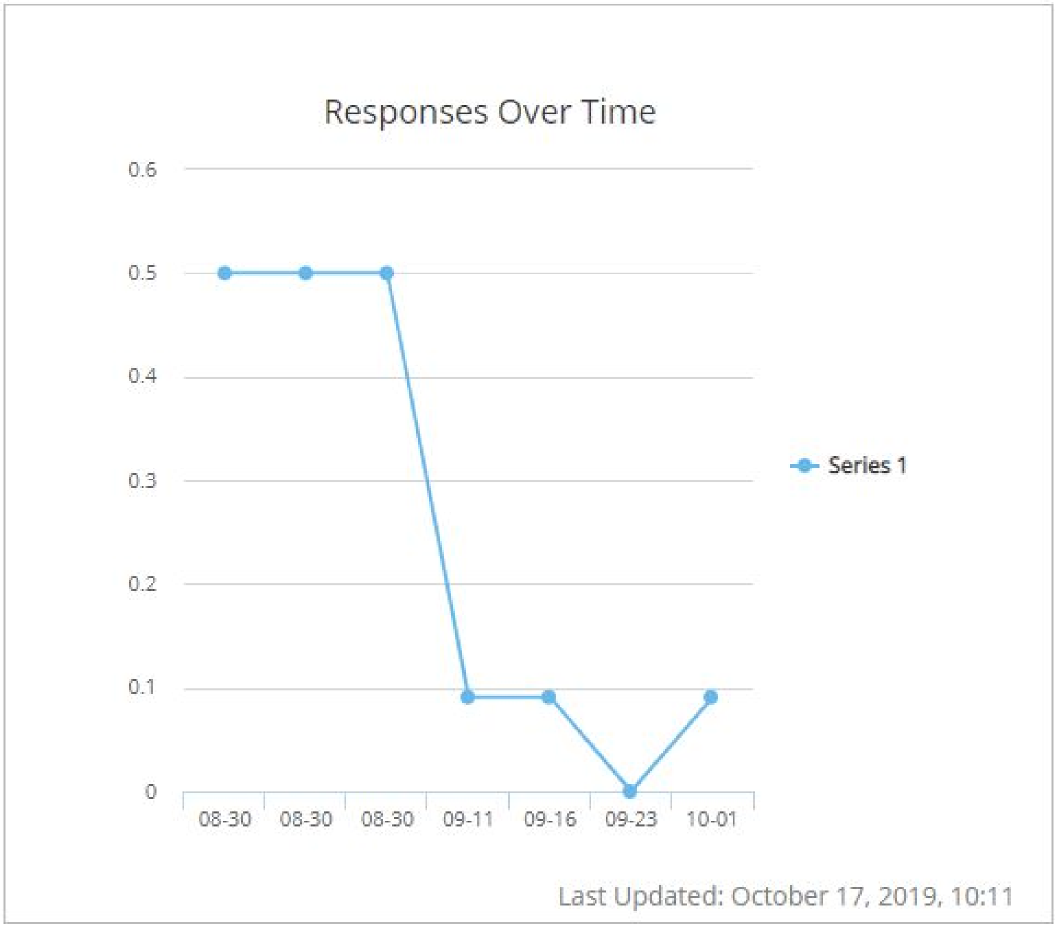
VMC Phishing Report July-September 2019

October 17th, 2019

Overview

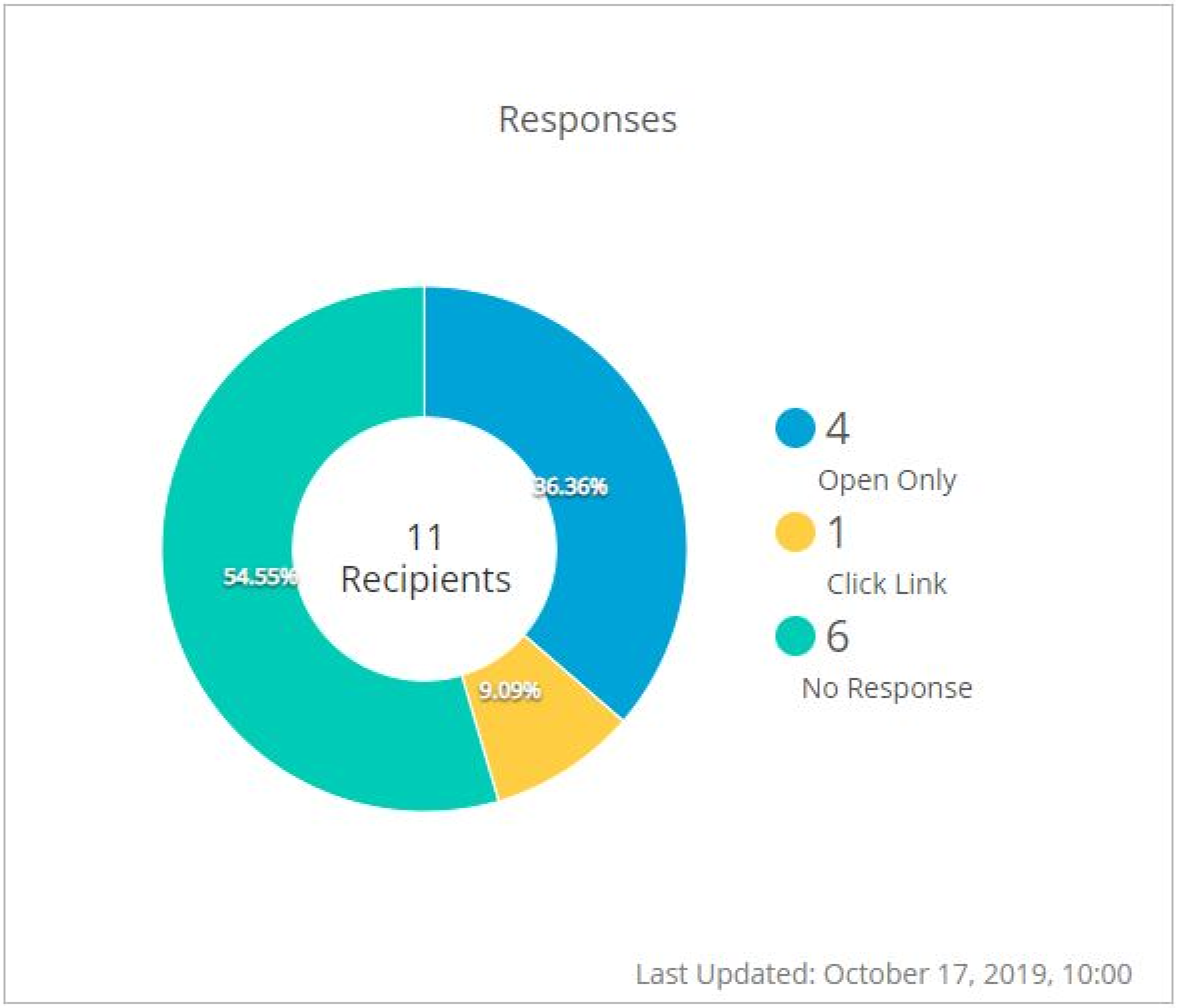
The quarterly phishing exercise involved sending out four separate phishing emails. The first phishing email was the most successful, with one employee not only clicking on the phishing link but also submitting information to a simulated phishing site! However, after the initial phishing email, employees behavior changed noticeably as seen in the summary graph here:



Campaign #1: Facebook Data Breach

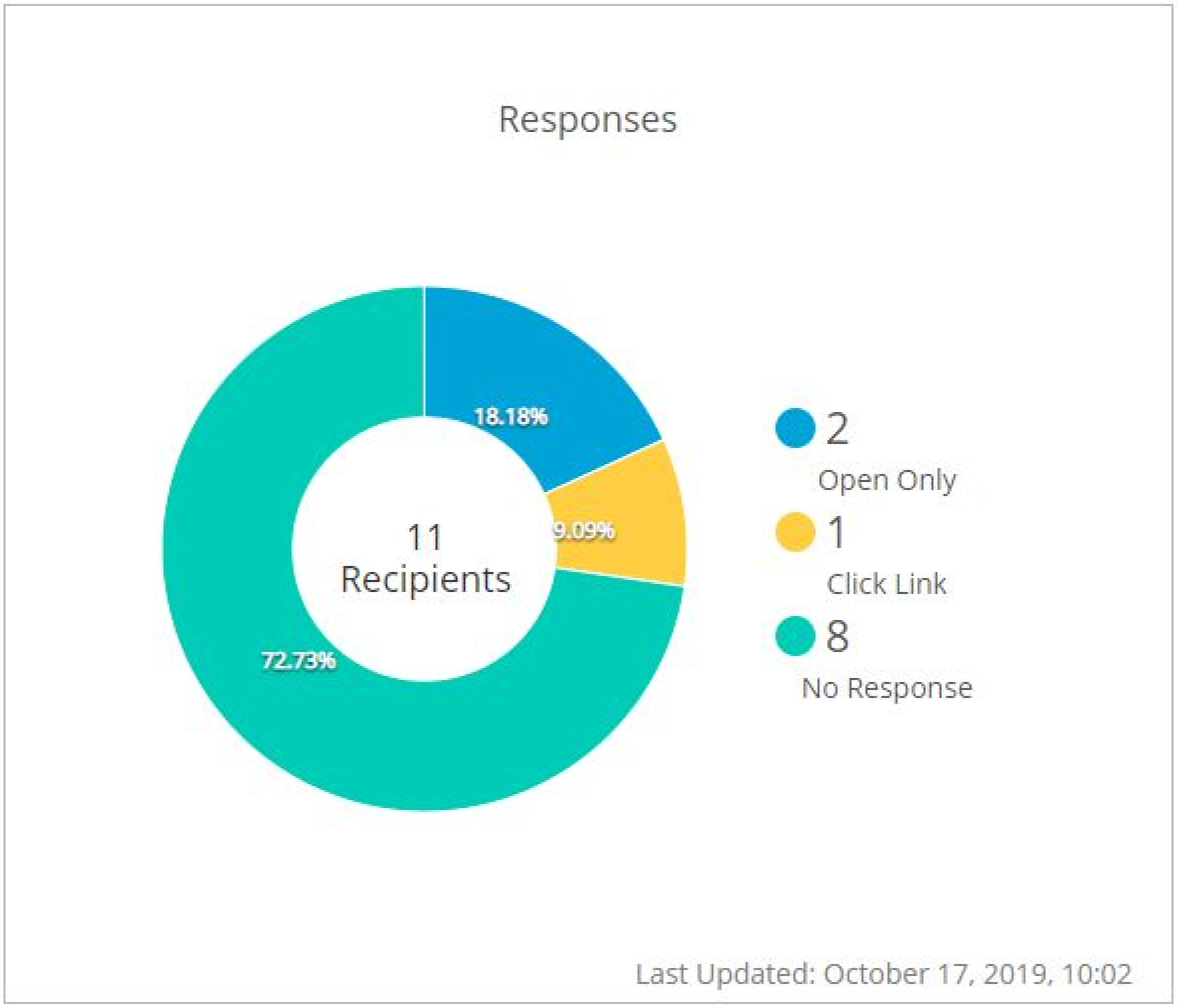
This phishing email campaign simulated a notice from Facebook about a data breach, prompting users to log in with their personal Facebook account information.

This campaign got one employee to not only click the link but submit personal data!



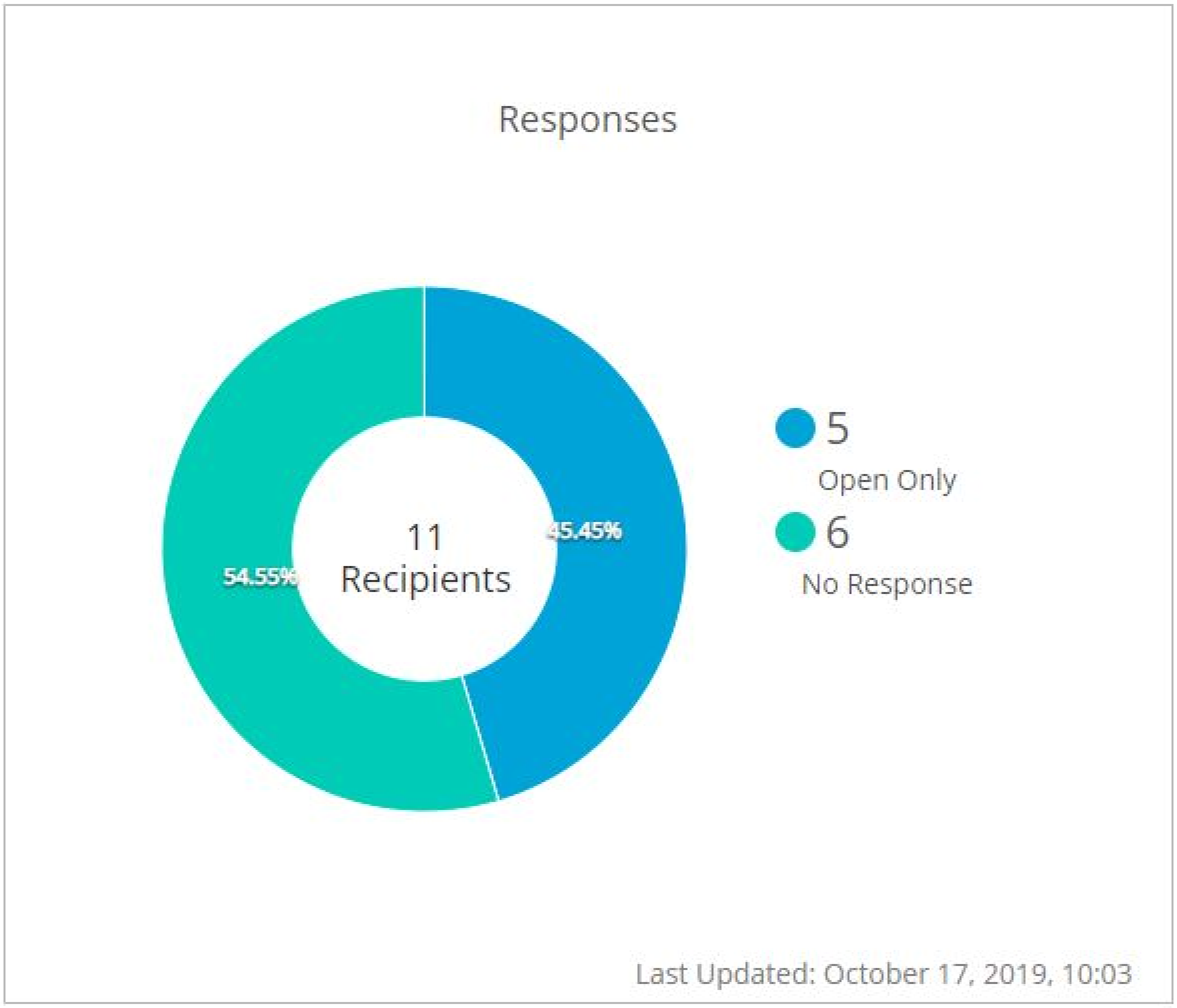
Campaign #2: Twitter Account Suspended

This phishing email campaign simulated a notice from Twitter about the user's account being suspended. One employee clicked on the link from the email, but did not submit personal information to the site.



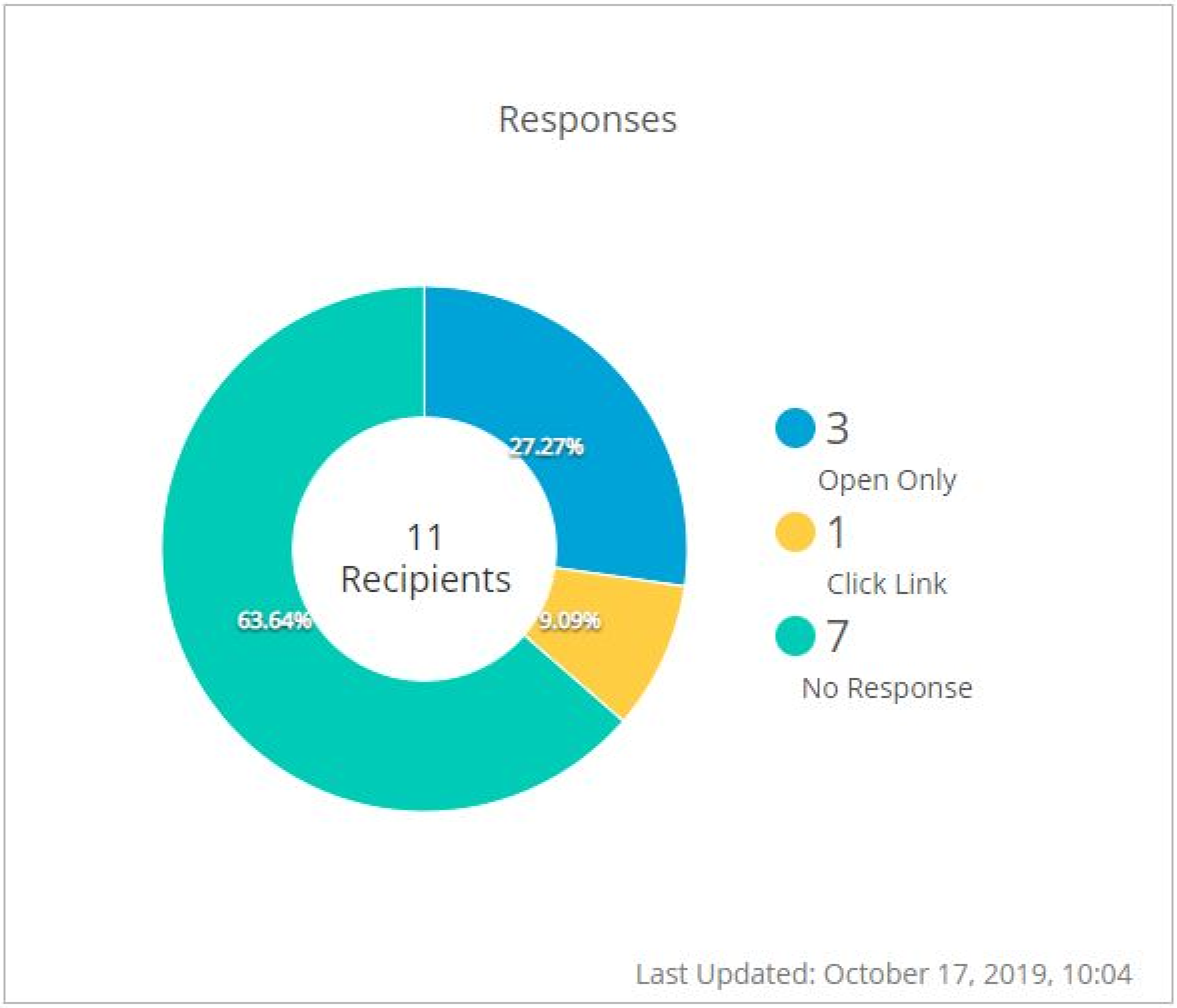
Campaign #3: Zoom Update

This phishing email campaign simulated a notice from the popular video conferencing site Zoom about a bogus update to their software that required a user's attention. Nobody at VMC clicked the link for this email!



Campaign #4: Credit Card Suspended

This phishing email campaign simulated a notice from the user's credit card company about their credit card being suspended. One user clicked the link, but did not submit personal information to the site.



Last Updated: October 17, 2019, 10:04