Hey y’all! During a recent risk management meeting at my company, we discussed ways to improve our overall security posture. One major area we agreed needed attention was phishing awareness. After some thorough research, I discovered a tool called GoPhish — an open-source phishing simulation platform.

Since this was my first time hosting an application on a Linux server, getting everything configured was a challenge. In particular, figuring out the correct certificate and key paths in the config file had me stumped for a while (you’ll see a screenshot of that config below). But after some trial and error, I finally got GoPhish up and running!

The second image shows the GoPhish login screen once everything was working. I went a bit overboard creating email templates — I found several GitHub repositories with templates I customized to fit our needs.

One interesting thing I noticed: when a user clicked a phishing email and landed on the mock Microsoft sign-in page, they would enter their info, and then get redirected to a 404 error page. To improve this, I designed my own landing page hosted on the same server that redirects users to an educational page explaining phishing and how to recognize it.

The next image shows my custom phishing awareness webpage. Finally, the next screenshot is from my first campaign — I made it way too easy the first time because I wasn’t sure how this was going to work, and wanted to test the waters. And for gigs I a little big of code from my landing page.