

Don't Get Hooked! Understanding Phishing

Students: Michaela Dunston, Eduardo Chung, Mario Vega & Alejandro Arrocha

Mentor: Dr. Masoud Sadjadi

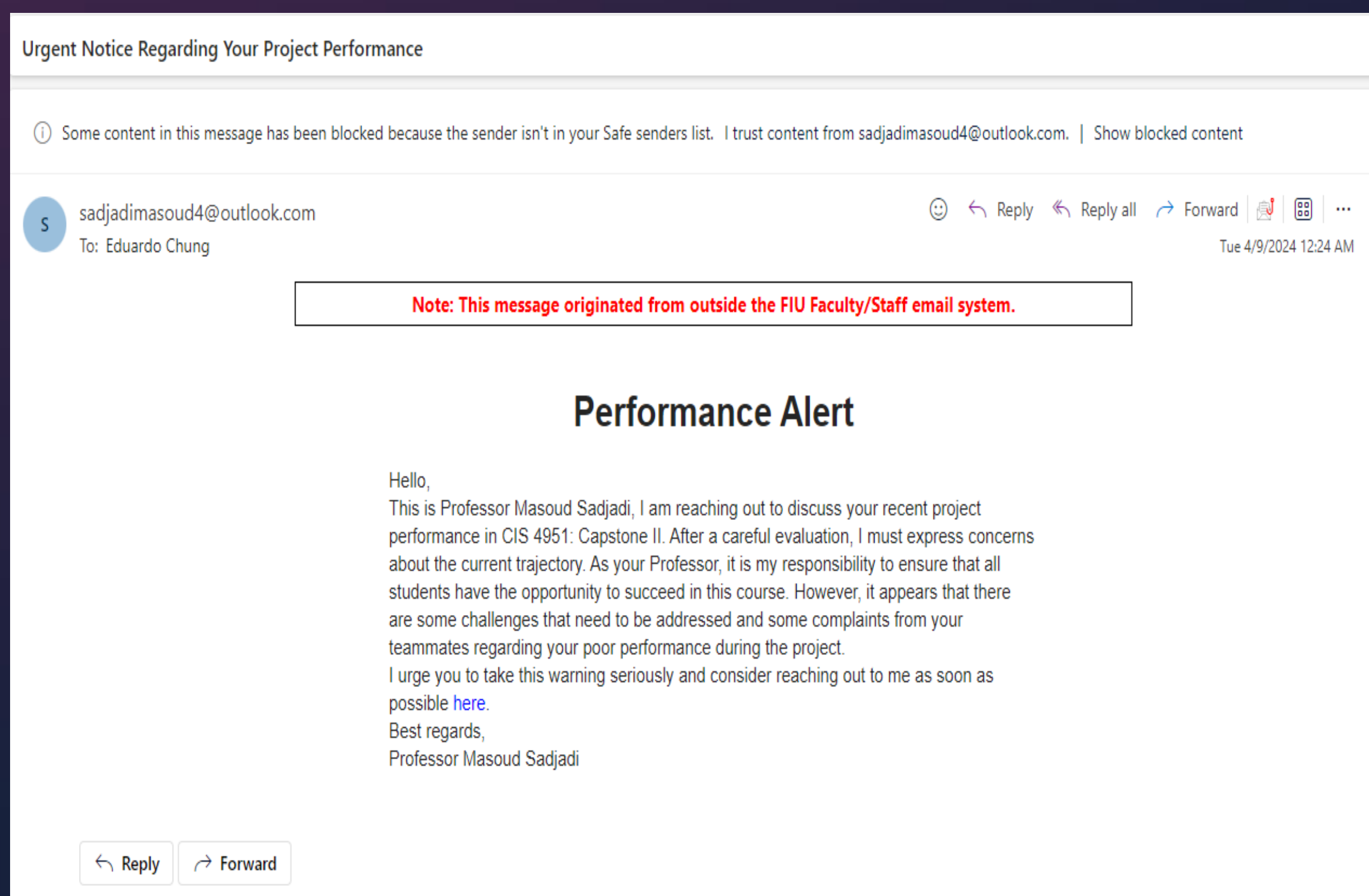
Instructor/Faculty: Dr. Masoud Sadjadi, Florida International University



Overview

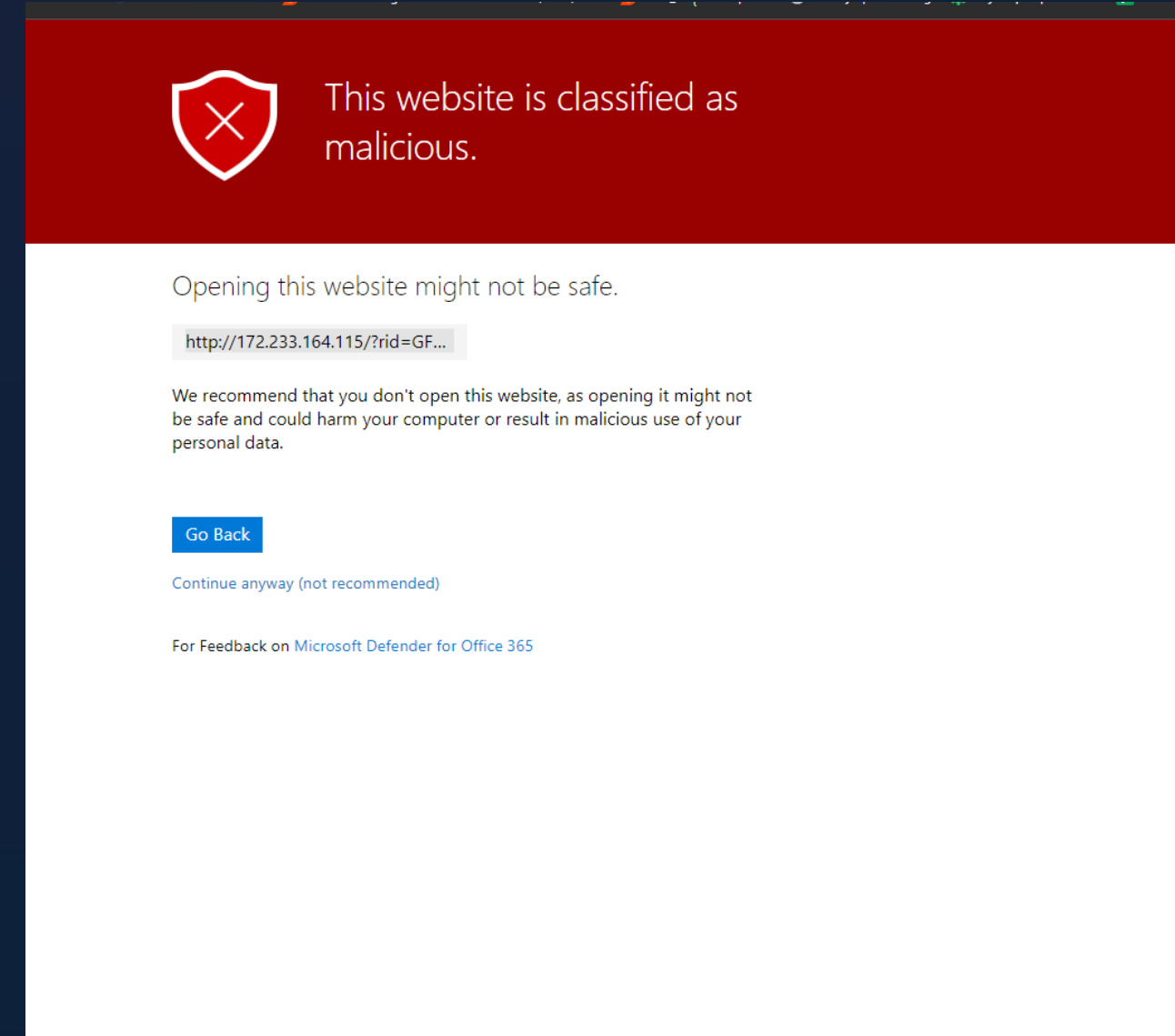
As previously discussed, the set up for the phishing campaign can be done quite easily and we can start gathering data. This in turn bring us some other issues that I can show below.

Email sent successfully

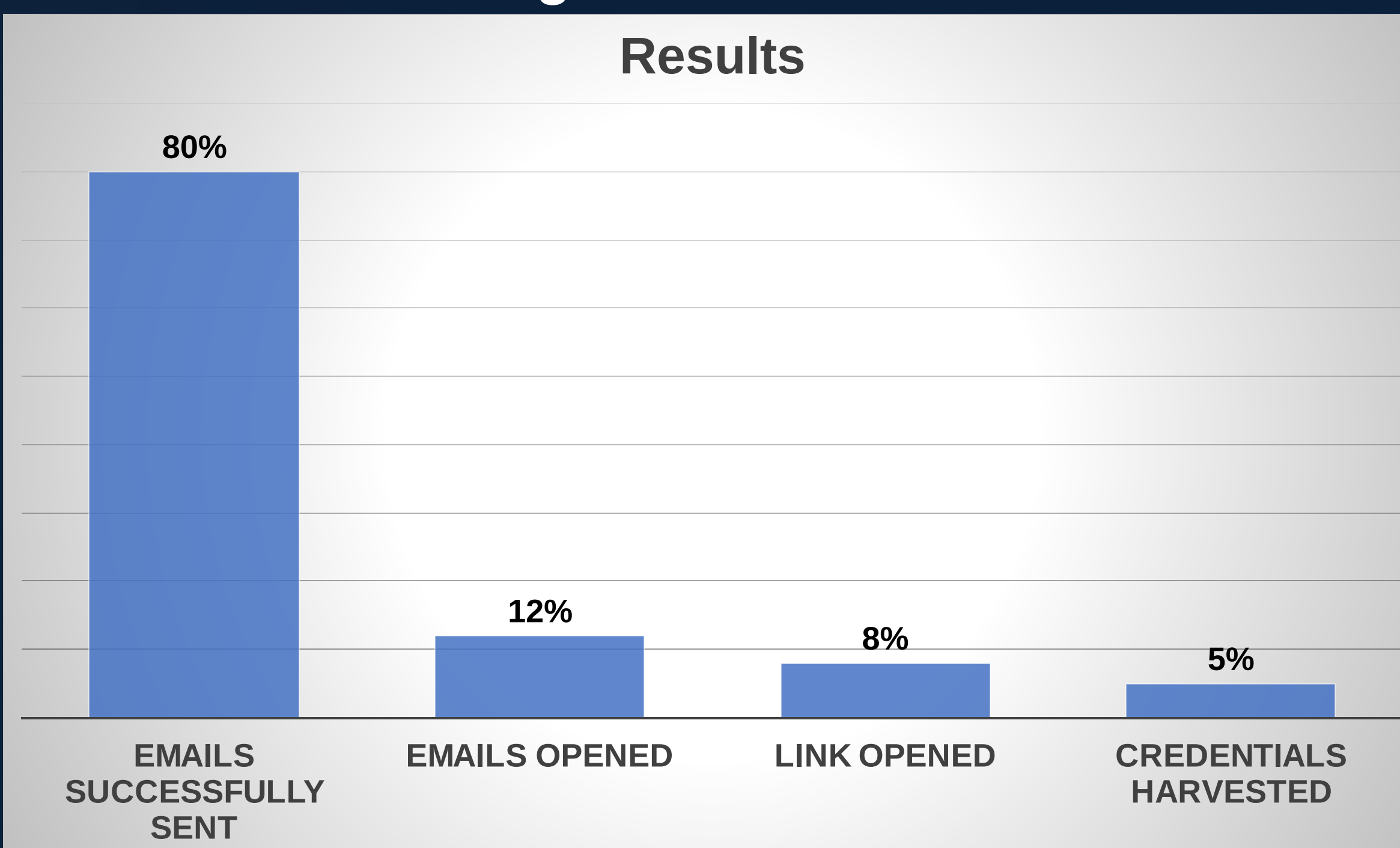


Issues

Mass Emails lead to blocks and bans from email server providers.



Results from testing

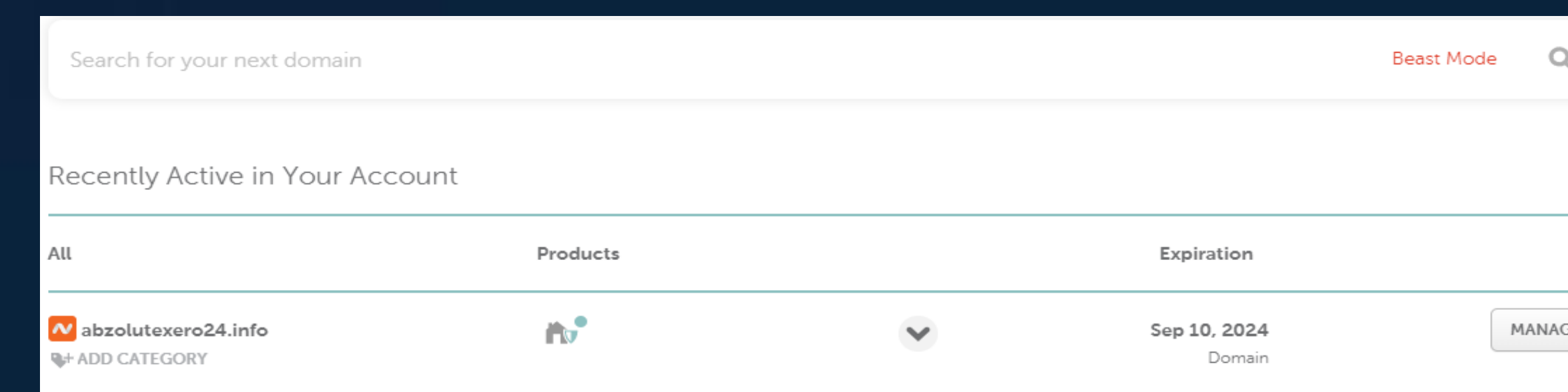
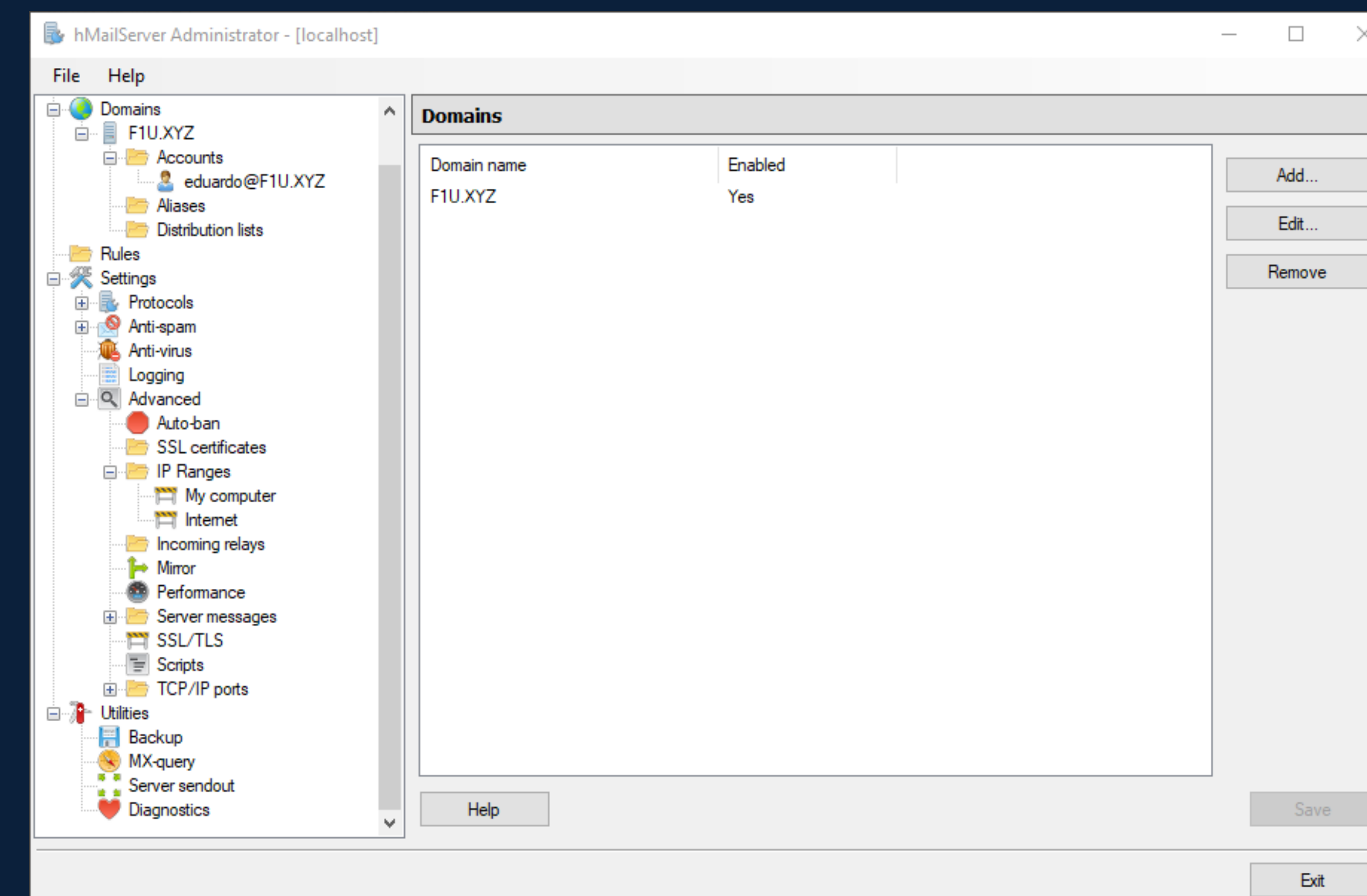


- Sample Size: 25
- Successfully sent: 80%
- Email Opened: 12%
- Link Opened: 8%
- Credentials harvested: 5%

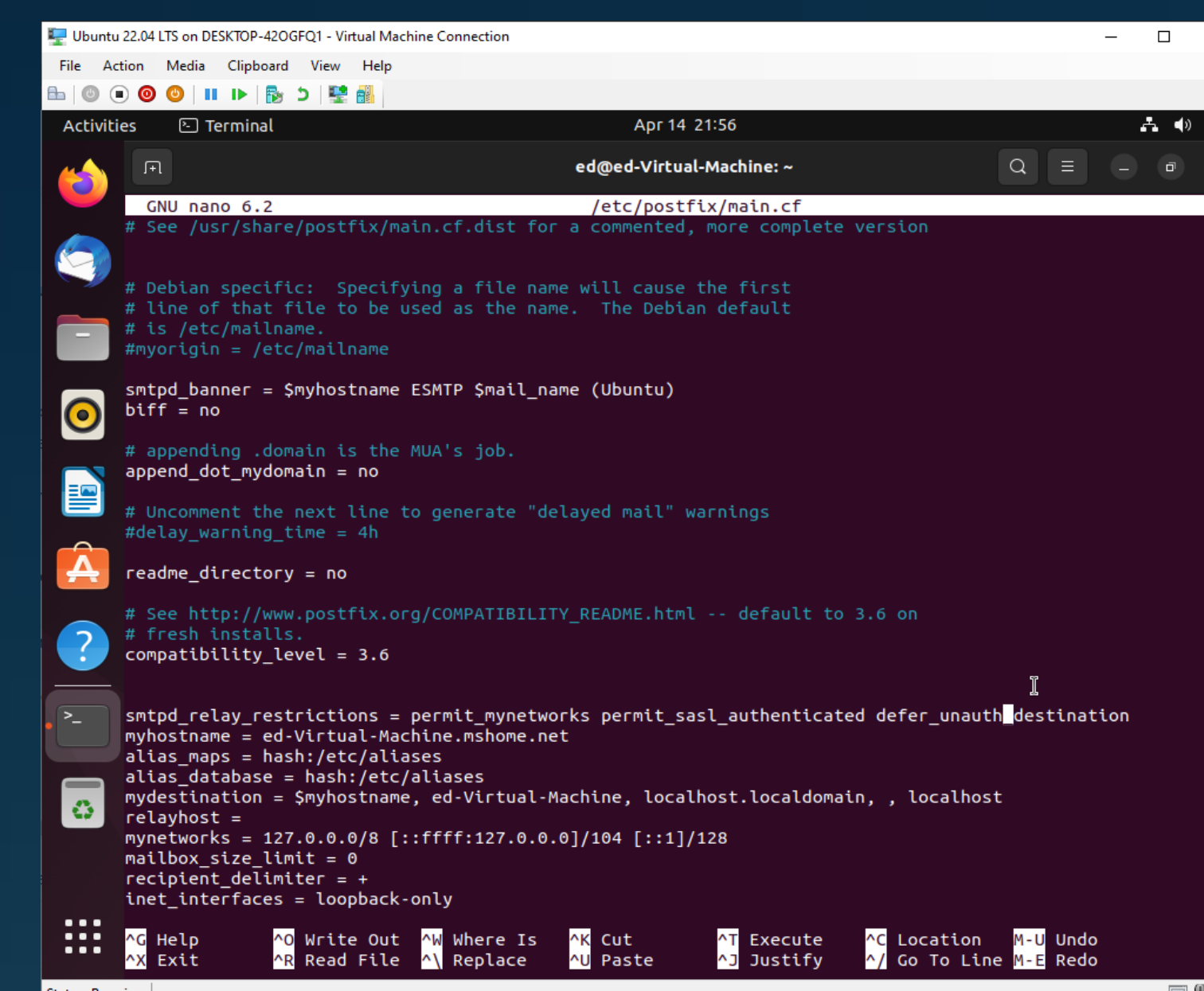
Conclusions

With GoPhish, we were able to set up and start properly testing a campaign to gather the data and put into perspective just how necessary this type of trainings truly are. The biggest issue we found that modern email providers will figure out what activity is happening and block accordingly.

STMP servers



The creation of a personal Mailing server can overcome the issue of commercial server bans and blocks



REFERENCES: <https://docs.getgophish.com/>, <https://www.hmailserver.com/>, <https://mailtrap.io/blog/setup-smtp-server/#How-to-setup-SMTP-mail-server-on-Linux>, <https://www.postfix.org/>

ACKNOWLEDGEMENT

The material presented in this poster is based upon the work supported by the Knight Foundation School of Computing and Information Sciences We/I thank Dr. Sadjadi for his/her/their assistance and mentorship that I/we received throughout the senior design project.