Phishing for Fun

By Madeline M. Moran
Email: mmoran11@luc.edu

Abstract: Perform a phishing experiment to see how many people fall victim.
This study was approved by the Loyola IRB

Step One: Survey
We conducted a paid survey advertised on Facebook that assessed participants:
- Knowledge of or experience with phishing emails
- Their thinking styles (intuitive, systematic, anxiety level, decision making)
- If they utilized any protective strategies (update regularly, check email sender)
- If they had vulnerable practices (reuse passwords, share passwords)

From this survey we collected their email. Each participants was compensated $3.

Step Two: Creating Phishing Material
We created a phishing email and website to send out to participants which claimed to be for a Covid-19 lottery to win 10,000 dollars

Email

Hello!

To meet the vaccination goal set by President Biden, the White house has announced a National Covid Vaccine Lottery for those who have received the vaccine.

Everyone who has had their Covid Vaccine can enter and will be eligible for a chance to win $10,000. 10,000 winners will each receive $10,000.

Click Here Now, to enter the lottery so you don't miss out!! Good luck!

PS: This link is unique to you; please do not share.

Website

Please provide the following information to be entered into the National Covid Vaccine Lottery:

Name:

Date of Birth:
mm/dd/yyyy

Last Vaccine Appointment Date:
mm/dd/yyyy

Vaccine Type:
Moderna

Last 4 Digits of Driver License:

State Associated with Drivers License:

Submit

Step Three: Logging activity
In order to gauge each individual's level of interaction with the phishing scam we had to be able to determine if they had clicked on the email, clicked on the link to the website, and if they had attempted to submit their personal information to the site. In each phishing, we embedded an invisible (1x1 pixel) image with a unique image name.

```
#looked at email
if "Trackers" and ".png" in request_path:
        start = '/Lottery/Trackers/'
        end = '.png'
```

```
#Clicked sumbit
elif "Submit" in request_path:
        start = '/Lottery/Submit/'
        end = ''
```

```
#clicked on link to website
elif "Submit" not in request_path and "Trackers" not in request_path:
        start = '/Lottery/'
        end = ''
```

Step Four: Authenticity
We struggled to get our Gmail account, and subsequently our Python program, to be recognized as legitimate rather than spam. We resolved this issue by implementing SPF, DKIM, and DMARC which gave our program authenticity enough to appear in inboxes.

SPF – Defines what mail servers can send through our domain. This allows us to define our servers IP address as a safe domain to send out emails
DKIM – Provides a digital signature on to each email to allow recipient servers to verify its authenticity. This helps prevent our email from being labeled as spam.
DMARC – If the email is still caught in spam filters despite SPF and DKIM, DMARC provides instructions for recipient servers on what to do with the email. In this case it allows us to tell other servers not to filter our email.

Step Five: Participant Interaction
We initially sent out our first phishing email to all participants on October 29th along with their virtual gift card to ensure they were looking at their email. We then sent out a secondary email 2 weeks later with a more urgent message 'Don't Miss Out!' to see if more people would respond. Finally, 2 weeks after our final phishing attempt, we sent all participants a debriefing message explaining the purpose of the survey.

Results:
Out of 597 participants who took the survey:
28.3% viewed the phishing email.
13.6% of those who viewed the email clicked on the link to the website.
56.5%% of those who went to the website would have submitted their information to the site.
In the future we will attempt to discern if there is any relation between the survey results and the phishing experiments results.

A Special Thank You to Anna Hart for her help with the survey as well as the Mulcahy Fellowship, an ORS Research Support Grant, and NSF DGE-1918591 and DGE-1919004 for funding this research.