

# An Experiment on Why You Are Vulnerable To Online Phishing Scams

Madeline M. Moran, Anna Hart, Mentors: Eric Chan-Tin, Loretta Stalans, Shelia Kennison

A Special Thank You the Mulcahy Fellowship, an ORS Research Support Grant, and NSF DGE-1918591 and DGE-1919004 for funding this research.

## Abstract

Phishing is a cyber-attack that uses deception to obtain personal identifiable information from individuals or corporations. These attacks are disguised as trustworthy sources, such as a bank, and convey an urgent situation that the recipient 'must' address through providing PII. Recipients are told to click on a link that provides a fraudulent website to enter PII and/or download malicious malware. Phishing attacks were the number one reported internet scam in 2022 and accounted for \$52 million reported loss [1]. The total amount lost to these scams increased by 48% [1] suggesting that scammers are adapting their phishing scams to increase revenue. Our research questions were: What personal characteristics increase vulnerability to phishing and how might that information inform new measures to spread phishing attack awareness and to prevent successful phishing attacks?

## Method

Participants (N = 584) completed a questionnaire with standardized scales on generalized anxiety, protective or vulnerable strategies, and decision-making styles. Four weeks later respondents received compensation of \$3 and received a phishing email containing embedded code to capture whether it was opened and whether the link was clicked. The phishing email and gift card were sent out at the same time to increase the chance of opening the phishing email. We were able to track participation through our server logs hosting the email and website and ensured we avoided collecting any personal information about the participants. The outcome variables were: whether they opened the email, clicked the link, and or clicked submit on the website. For those who opened the email, we examined the correlations between their psychological profile and if they were phished.

## Phishing Example

### EMAIL:

- The email is from 'vaccine@nationallottery.com'.
- There is a slight misspelling that participants may find suspicious: an added 'l' between 'national' and 'lottery'.
- This email claims to be part of an initiative with the US White House, however there are no official seals included nor any particular branch or initiative singled out by name.

### WEBSITE:

- 'http://nationallottery.com/Lottery/'

## Survey

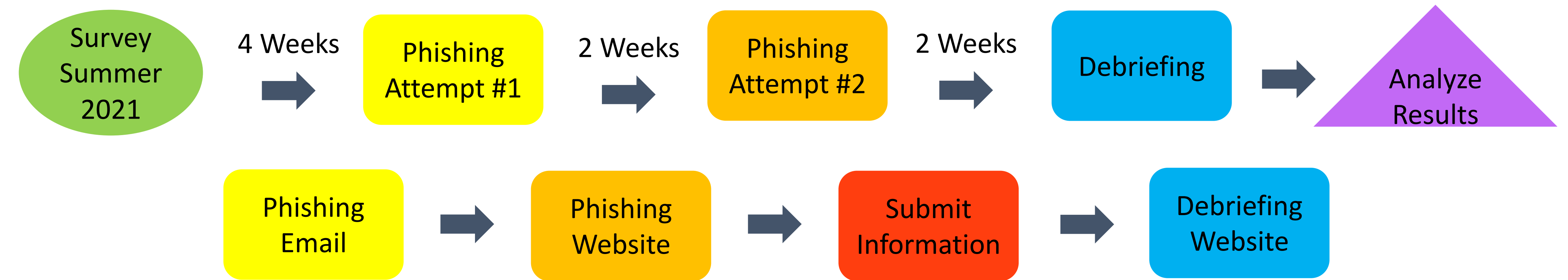
The survey included:

- Knowledge of or experience with phishing emails.
- Thinking styles (intuitive, systematic, anxiety level, decision making).
- Utilization of any protective strategies (update regularly, check email sender).
- Vulnerable strategies (reuse passwords, share passwords).
- Emails were voluntarily collected as a method of providing compensation.

Facebook Ad:  
Fill out this 25-minute survey from Loyola University Chicago about your experiences post COVID-19 and get compensated with \$3. Adults who regularly check email, live in USA, and received COVID vaccine are eligible.



## Procedure



## Email Code

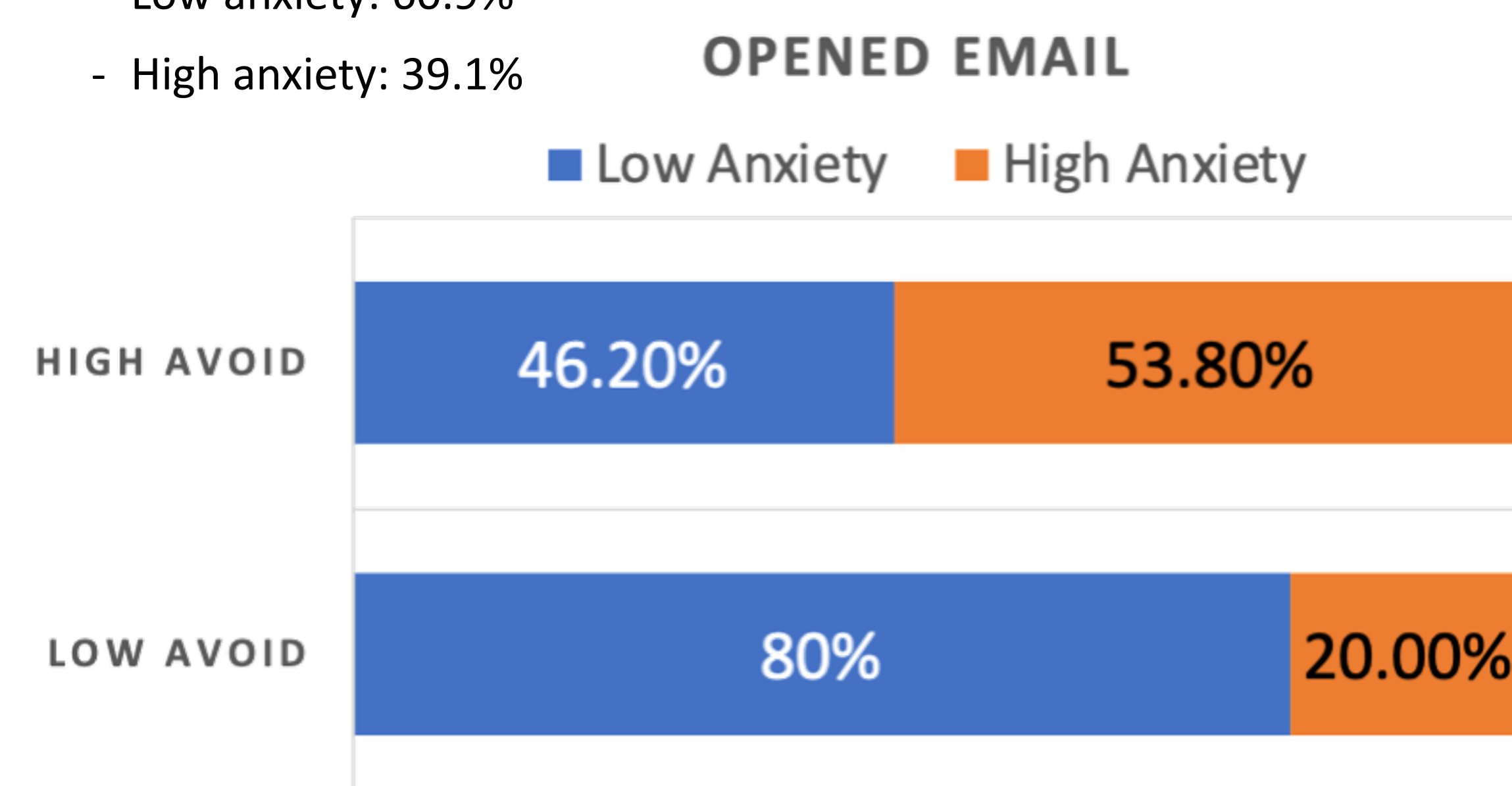
```
hashobject = base64.b64encode(toaddr.encode("utf-8"))
email = x
email = email.strip()
Hash_File.write(email + " : " + hashobject.decode("utf-8") + "\n")
shutil.copy2('/var/www/html/Lottery/Trackers/1x1.png',
            '/var/www/html/Lottery/Trackers/%s.png' % hashobject.decode("utf-8"))
...

<input type="text" name="driver" id="driver"><br><br>
State Associated with Drivers License: <br>
<input type="text" name="state" id="state"><br><br>
<button type="submit" value="Submit" onclick="myFunction()">Submit</button>
<script>
function myFunction() {
var x = location.href;
x = x.substring(36, x.length);
x = "https://nationallottery.com/Lottery/Submit/"+x;
```

- No information was collected from the site to not compromise participants' privacy.
- After clicking the button, they were taken to a loading screen followed by the debriefing site.

## Results

- Out of 584 legitimate participants, 28.3% viewed the phishing email.
- Of those who opened the email, 13.6% clicked on the link.
- 56.5% clicked submitted to the website.
- Characteristics of the 153 participants who opened the email:
  - Vulnerable strategies: 78.3%
  - Low anxiety: 60.9%
  - High anxiety: 39.1%



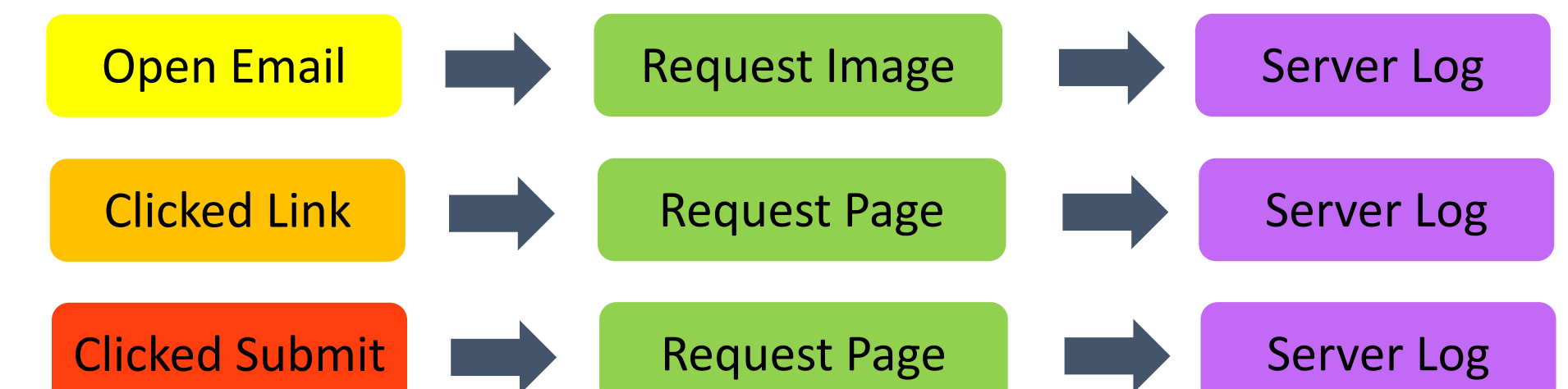
## Log Parser and Hash Codes

[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.

https://nationallottery.com/Lottery/bW1vcmFuMTFAbHVjLmVkdQo=

bW1vcmFuMTFAbHVjLmVkdQo=



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

#Clicked submit
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 = ''
```

- Each participant was assigned a unique hash code as a means of anonymous identification.
- Unique hash code is linked to the survey data.

## Programs Used

- Python: Log parser and Email
- Apache: Website
- HTML: Email and Website
- JavaScript: Website



## Conclusions and Limitations

- Hypothesis: Those with higher anxiety would be more likely to click on the email. In similar experiments this has proven true when focused on loss.
- Our results were in the opposite direction. But this may be confined to emails focusing on gains.
- Limitations:
  - Participants were collected from Facebook.
  - They were not vetted or regular survey participants.
  - We could not verify any information they provided.
  - Only 28.3% of participants opened the phishing email.
- Conclusions:
  - We were able to create and deploy a phishing scam from our own server using python and Gmail.
  - Of those who saw the email, 61% scored low on the general anxiety scale.
  - Of those who visited the website, over half tried to submit vulnerable information.

[1] "Internet Crime Complaint Center Releases 2022 Statistics." FBI, FBI, 22 Mar. 2023, <https://www.fbi.gov/contact-us/field-offices/springfield/news/internet-crime-complaint-center-releases-2022-statistics>.