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 thorough 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?

Procedure

Survey Summer 2021
4 Weeks Phishing Attempt #1
2 Weeks Phishing Attempt #2
2 Weeks Submit Information
Debriefing
Analyze Results

Email Code

```
hashobject = base64.b64encode(hashlib.md5('utf-8').encode)
email = +
email = email.strip()
hashed_file.write(email + ‘; ‘ + hashobject.decode(‘utf-8’) + ‘; ‘ + email
print(shutil.copy2(’/var/www/html/LotteryTrackers/list.png’,
’/var/www/html/LotteryTrackers/ha.png’)
+ hashobject.decode(‘utf-8’))
...)
```

Log Parser and Hash Codes

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

Website Code

```
Last 4 Digits of Driver License(s):
<input type="text" name="driver" id="driver"/>
<br>
State Associated with Drivers License: <br>
<input type="text" name="state" id="state"/>
<br>
<button type="submit" value="Submit" onclick="myFunction()">Submit</button>
```

- 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%

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.