User Study on User Behavior and Susceptibility to Phishing Attacks on Mobile vs Desktop Platforms

Venkata Subrahmanya Abhinav Rallapalli
The University of Texas at Arlington
Arlington, Texas, United States
sxr8961@mavs.uta.edu

Vishal Reddy Vancha
The University of Texas at Arlington
Arlington, Texas, United States
vxv6184@mavs.uta.edu

Sivani Tumuluri
The University of Texas at Arlington
Arlington, Texas, United States
sxt8984@mavs.uta.edu

ABSTRACT

Phishing attacks remain a significant threat to cybersecurity, with attackers increasingly targeting mobile device users. This project aims to conduct a user study to analyze users' behavior and susceptibility to phishing attacks on mobile and desktop platforms. By focusing on both platforms, we seek to identify differences in user responses and vulnerability factors. Our research questions include investigating how demographics, education, and awareness influence susceptibility to phishing. Through this study, we aim to contribute valuable insights to the field of cybersecurity and improve strategies for mitigating phishing threats.

ACM Reference Format:
Venkata Subrahmanya Abhinav Rallapalli, Vishal Reddy Vancha, and Sivani Tumuluri. 2024. User Study on User Behavior and Susceptibility to Phishing Attacks on Mobile vs Desktop Platforms. In *Proceedings of Did not publish (Not Published).* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

1.1 Introduction

Phishing attacks still continue to pose a significant threat to individuals and organizations worldwide to this day. With the proliferation of mobile devices and the increasing reliance on them for various online activities, mobile users have become prime targets for phishing attacks. This project seeks to address the gap in existing research by conducting a user study to analyze the behavior and susceptibility of users to phishing attacks on both mobile and desktop platforms. The importance of this study is underscored by the growing sophistication of phishing attacks, which often exploit users' trust and familiarity with digital interfaces. By understanding how users interact with phishing attempts on different platforms, we can identify key factors that influence their susceptibility. Through this study, we aim to contribute valuable insights to the field of cybersecurity and inform the development of more effective measures to combat phishing attacks. By raising awareness about phishing threats and promoting best practices for online security, we hope to empower users to protect themselves against these pervasive and evolving threats.

1.2 Motivation

The motivation behind this project stems from the increasing prevalence and sophistication of phishing attacks, which pose a significant threat to individuals worldwide. While there are security measures and awareness campaigns aimed at mitigating these attacks, there is a need for a deeper understanding of user behavior and susceptibility to phishing across different platforms, particularly mobile and desktop devices. By conducting a comprehensive user study, we aim to gain insights into how users perceive and respond to phishing attacks, identify factors that influence their susceptibility, and ultimately enhance cybersecurity awareness and defenses against such threats.

1.3 Objectives

- Assess user behavior and susceptibility to phishing attacks on mobile devices and desktops.
- Compare user responses to phishing attacks on mobile devices versus desktops.
- Determine the susceptibility of participants to phishing attacks on mobile devices compared to desktops.
- Investigate the influence of demographics (age, gender, occupation) on user susceptibility to phishing attacks.

1.4 Research Questions

(1) How do participants' demographics, such as age, gender, and occupation, influence their susceptibility to phishing attacks on mobile and desktop platforms?
(2) To what extent does education and awareness about phishing attacks and cybersecurity impact participants' behavior and susceptibility to phishing attacks on mobile and desktop platforms?
(3) What are the main differences in user behavior and response patterns to phishing attacks between mobile and desktop platforms, and how can these differences inform cybersecurity strategies?

1.5 Hypothesis

H1: Users are more likely to engage with phishing links when using mobile devices compared to desktop platforms.
  a. Users using mobile devices are more likely to not identify the phishing links.

Not Published, May 05, 2024, Arlington, TX

ACM ISBN 978-x-xxxx-xxxx-x/YY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

b. Users using mobile devices are more likely to not submit credentials on phishing websites.
c. Users using mobile devices are more likely to look for different features on phishing websites.

2 PREVIOUS WORKS

In our literature survey, we primarily divided our focus into two categories: papers related to phishing and papers related to user studies in cybersecurity. We made this division due to the limited number of papers that comprehensively cover both topics, especially in the context of phishing on mobile devices. Most of the existing literature analyzes phishing attacks in general, with limited focus on the specifics of mobile devices. Conversely, some papers delve into user studies in cybersecurity, offering insights into user behavior and responses to security threats. However, there is a noticeable gap in the literature when it comes to integrating both areas and conducting in-depth studies on phishing attacks on mobile devices. Several studies have investigated user behavior and susceptibility to phishing attacks, as well as the effectiveness of anti-phishing tools, but there is limited research comparing phishing attacks on mobile and desktop platforms. However, in [10], where researchers compared mobile and desktop phishing attacks, researchers found that users are more likely to click on phishing links when they are visually obscured, such as when displayed as buttons or masked as text, compared to when shown as URLs more actively on mobile devices than desktop platforms. However, the hypothesis was supported by a very small effect size, indicating that its significance may be limited. Most papers included data analysis on phishing and phishing attacks in general while other papers did user studies. Through our review of the literature, we have gained valuable insights into phishing attacks and their various types. We have learned about the factors that make certain users susceptible to phishing attacks, as well as the methods used by attackers to carry out phishing campaigns, particularly through emails. We have also explored the different types of links used in phishing emails, including raw links, buttons, and hypertext. Additionally, we have come across research discussing the potential use of AI in generating phishing attacks [7] , which aligns with our future plans to develop AI-generated phishing attacks for our study. Our project differs from existing studies in several key aspects. Firstly, while many studies have focused on either phishing attacks or user studies in cybersecurity, we aim to bridge the gap between these areas by conducting a comprehensive user study specifically focusing on phishing attacks on mobile devices. This targeted approach allows us to gain a deeper understanding of user behavior and susceptibility to phishing attacks in a mobile context, which is becoming increasingly relevant due to the widespread use of smartphones and tablets. Secondly, our project involves a comparative analysis of phishing attacks on mobile and desktop platforms. While some studies have examined phishing attacks on one platform or the other, few have directly compared the two. By analyzing the differences in user behavior and response patterns between mobile and desktop platforms, we can identify unique challenges and vulnerabilities associated with each platform and develop targeted strategies to mitigate these risks. Overall, our project offers a unique and comprehensive approach to studying phishing attacks on mobile devices, with a focus on user behavior, comparative analysis, and awareness-raising initiatives.

3 METHODOLOGY

This user study was conducted as a prototype with a small number of participants, primarily our classmates. The purpose was to gain insights into how to conduct the study on a larger scale in the future. While we initially considered seeking IRB approval for this study, we ultimately decided against it since it was a prototype involving a limited sample size. However, for any future larger-scale studies, we plan to obtain IRB approval. To prepare for this, all authors completed the required HSP training and obtained certificates. We also filled out an IRB application form, detailing all necessary documents and providing answers to relevant questions. However, we did not submit the application, as we first wanted to conduct the prototype study to better understand the experiment's dynamics, in alignment with our mentor's guidance.

3.1 Participant Gathering

We conducted a prototype study for this project which included participants from our class and our professor's lab students. we recruited participants from diverse backgrounds, including different demographics (age, gender, occupation) and levels of cybersecurity awareness. Participants are primarily the students in UTA. Participants are recruited through email services. A participant receives an email with the link to the consent form and the Question Pro platform on which the whole experiment is hosted. Participants are split into two groups – participants for mobile devices and desktop platforms and each group participant receives the designated Question Pro survey link based on their device. The Question Pro platform records what device is being used and informs us. Participants are not required to provide any user credentials for the experiment. This way, no data of the participants is collected or used. Participants are split almost equally, that is, 6 participants for mobile platforms and 5 participants for desktop platforms. For both mobile and desktop platforms, the participant simply goes through the question pro survey.

3.2 Ethical Consideration

We ensured that the study is conducted ethically, with informed consent obtained from all participants before we begin our experiment, we also gave the user choice to opt out at any time they felt uncomfortable during the experiment. We protected participant privacy and confidentiality by anonymizing data and adhering to data protection regulations. We ensured that no personal user data or user credentials is being collected.

3.3 User Consent Form

The User Consent Form is attached in the next page.

Consent/Disclosure Form:

Title: Website Quality and Legitimacy Assessment Study Consent/Disclosure Form

Introduction:

Thank you for participating in our study on quality and legitimacy assessments of websites visited on various platforms, particularly mobile phones vs. desktop platforms. Before you proceed, please read the following information carefully.

Purpose of the Study:

The purpose of this study is to assess the quality and legitimacy of websites visited on mobile devices compared to desktops. Your participation will help us design higher-quality and more secure websites.

About high quality and legitimate websites:

These websites tend to have a clear purpose or mission, which is evident in their content and messaging. They prioritize transparency and authenticity, ensuring that their intentions and practices are easily understood by their users. Additionally, these websites often have a robust security infrastructure in place, including measures to protect against malware, phishing attacks, and other online threats. Overall, high-quality websites prioritize user trust and strive to maintain a positive reputation in the online space.

About illegitimate websites:

In addition to their poor design and deceptive tactics, illegitimate websites often pose serious security risks to users. Illegitimate websites are usually fake websites that attempt to deceive users into fraud or malicious attacks or to spread misinformation. Examples of such attacks are Denial of Service, Phishing, SQL injection, Ransomware, Trojan horse attacks etc. Phishing attacks are a form of social engineering in which attackers deceive users into revealing sensitive information. These attacks can be done through emails, text messages, or websites that look legitimate but are actually designed to steal your information.

Procedure:

You will be asked to participate in a survey hosted on Question Pro in your own environment. You will be requested to answer a few demographic questions along with general questions on about your knowledge and experience with high-quality, low-quality and illegitimate websites. Then, you will see multiple websites on the survey and will be asked to interact with the provided link. You need to assess each given website to see if it is of high quality or not. Some websites provided might not be high quality or malicious. **Please note that this is a simulation, and no real harm can come from clicking on the link**. Your actions and responses will be observed in the form of your answers for research purposes only. The observation and analysis of your responses are performed manually by the researchers actively after the experiment, and no third-party or software is being used to observe, record, store and share said data. **This data is not being shared with any third parties**. **NO actual user credentials are being used or collected.** You are then requested to answer a few post-experiment questions to discuss your experiment run.

Data Collection:

You will be assigned a participant number to anonymize any data we collect. During the study, we will collect information about your age, gender, occupation, education level, and other relevant demographics. We will also collect data on your responses to the websites. **Please be assured that your personal information will not be collected or shared with anyone.** All data will be anonymized and used only for research purposes.

How is this data used:

Demographic data like age, gender, occupation, education level, etc., will be used to generalize and group participants to observe similarities between them. The responses to the websites are used to perform quantitative and qualitative analyses and understand similar behavior patterns.

Confidentiality and Participant Rights:

Participant confidentiality is of utmost importance in this study. Your responses will be kept confidential, and your identity will not be linked to your data in any way. Your responses will be anonymized and aggregated for analysis, and no individual participant will be identified in any reports or publications resulting from this study. Only the research team will access to the data, and all data will be stored securely.

Your participation in this study is voluntary, and you can withdraw at any time without penalty. Your decision to participate or not will not affect your relationship with the researchers or the University in any way. If you have any questions or concerns about your rights as a participant, you can contact the researchers at any time for clarification.

Participant Consent:

By continuing with this study, you indicate that you have (1) read and understood the information provided about cyberattacks, (2) read and understood the information provided about the experiment procedure, (3) gave permission to the researchers to collect both demographic data and experiment data in an anonymized manner and, (4) understood that no personal user data is being collected or shared, and (5) non-disclosure of any collected data mentioned by the researchers and (6) voluntarily agree to participate.

If you have any questions or concerns, please contact the researcher listed below.

Researcher Contact Information:

Venkata Subrahmanya Abhinav Rallapalli	Vishal Reddy Vancha	Sivani Tumuluri
sxr8961@mavs.uta.edu	vxv6184@mavs.uta.edu	sxt8984@mavs.uta.edu
+1 (940)843-1222	+1 (469)394-7249	

Participant Signature:

____

(Signature)

Date:

____

Thank you for your participation. Your contribution is valuable to our research.

3.4 Environment and identifiable features

Desktop – Users are using their own desktop devices and their own browser. They are provided with a link to the experiment hosted in question pro platform though an email. Mobile – Users are using their own mobile devices and their own browser. They are provided with a link to the experiment hosted in question pro platform though an email. Same as the desktop platform participant goes through the survey and judges the websites. The difference between desktop and mobile platforms is that the change in the user experience and website design effecting the participant based on the platform and browser being used.

3.5 Pre Experiment survey

We gathered user demographics and their knowledge on cyber security. Basic cyber security knowledge questions are asked to determine the level of knowledge the participants have on cyber security. Additionally, the participants are asked to rate themselves on how knowledgeable they think they are. This can be used to draw a contrast on the false sense of knowledge they pretend on having.

3.5.1 Demographics. We asked the participant basic demographic questions like:

(1) Please state your age
  (a) Under 18
  (b) 18-24
  (c) 25-34
  (d) 35-44
  (e) 45-54
  (f) 55-64
  (g) Above 64
(2) Gender
  (a) Male
  (b) Female
  (c) Non-binary
  (d) Prefer Not to Say
  (e) Other ___________
(3) Please state your race
  (a) Hispanic or Latino
  (b) American Indian or Alaska Native
  (c) Asian
  (d) Black or African American
  (e) Native Hawaiian or Other Pacific Islander
  (f) Caucasian or White
  (g) Multiracial
  (h) Prefer not to say
  (i) Other ___________
(4) Highest level of education
  (a) High School
  (b) Associate's Degree
  (c) Bachelor's Degree
  (d) Master's Degree
  (e) Doctoral Degree

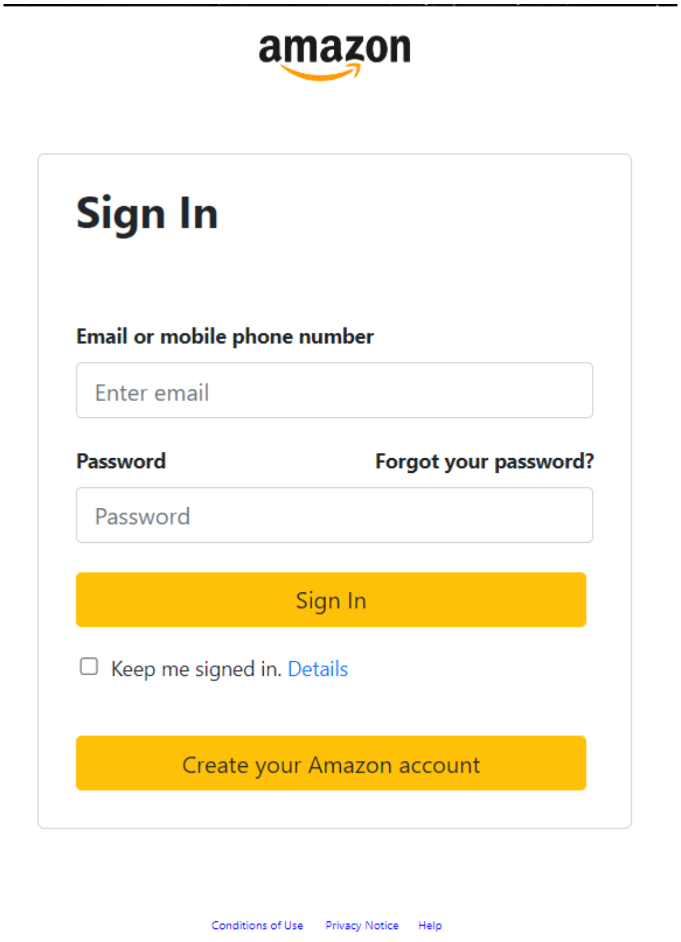
3.5.2 Basic Cyber Security Knowledge Questions. We then asked basic cyber security questions in order to understand the knowledge of the participant.

(1) How confident are you in identifying websites which might not be legitimate?
  (a) Not confident at all
  (b) Slightly confident
  (c) Moderately confident
  (d) Very confident
  (e) Extremely confident
(2) How often do you update your software and security settings on your browsers?
  (a) Never
  (b) Once a year
  (c) Once every 6 months
  (d) Once a month
  (e) Always
(3) How often do you encounter a suspicious website?
  (a) Never
  (b) Once a year
  (c) Once every 6 months
  (d) Once a month
  (e) Always
(4) Have you ever been a victim of an online scam in the last year? If yes, how many times?
  (a) 0
  (b) 1-2
  (c) 3-4
  (d) 5-7
  (e) 8-10
  (f) More than 10
(5) Have you received any formal cybersecurity training?
  (a) Yes
  (b) No
(6) What do you do when you encounter a website that looks suspicious to you?
  (a) Close the browser window.
  (b) Close the browser and run a scan on my system using my Antivirus.
  (c) Check for the link using one or more URL Scanning Tool.
  (d) Search for articles/forum posts about the website to see what others feel about it.
  (e) Other ___________
(7) Which devices do you use regularly for checking social media websites? (Select all that apply)
  (a) Mobile phone/Tablet
  (b) Laptop/Desktop computer
(8) Which devices do you use regularly for checking emails? (Select all that apply)
  (a) Mobile phone/Tablet
  (b) Laptop/Desktop Computer

3.6 The Experiment

After we split the users in two for the two devices, participants undergo Identification/distinguishment of high quality and not so high-quality websites. The user goes through all links provided and rate each website if it is high quality. The user will be provided with user credentials so we do not extract any user data. The participants will receive the links for the experiment through the question pro survey. (Note: 1 participant 1 device only). After each website, the participant is asked to answer a likely meter on how high quality the website is.

Not high-quality website samples: Facebook, Amazon, Instagram, Twitter (X). Screenshots of these sites developed by the researchers are attached below. Note: Only login pages are created using HTML/CSS and no data is actually collected or stored when clicked on buttons on the web pages. The web sites are self developed, which are developed using manual coding and other sources like codepen.io, geeks for geeks, GitHub. This is done to simulate the real-world attacks.



amazon

Sign In

Email or mobile phone number

Enter email

Password Forgot your password?

Password

Sign In

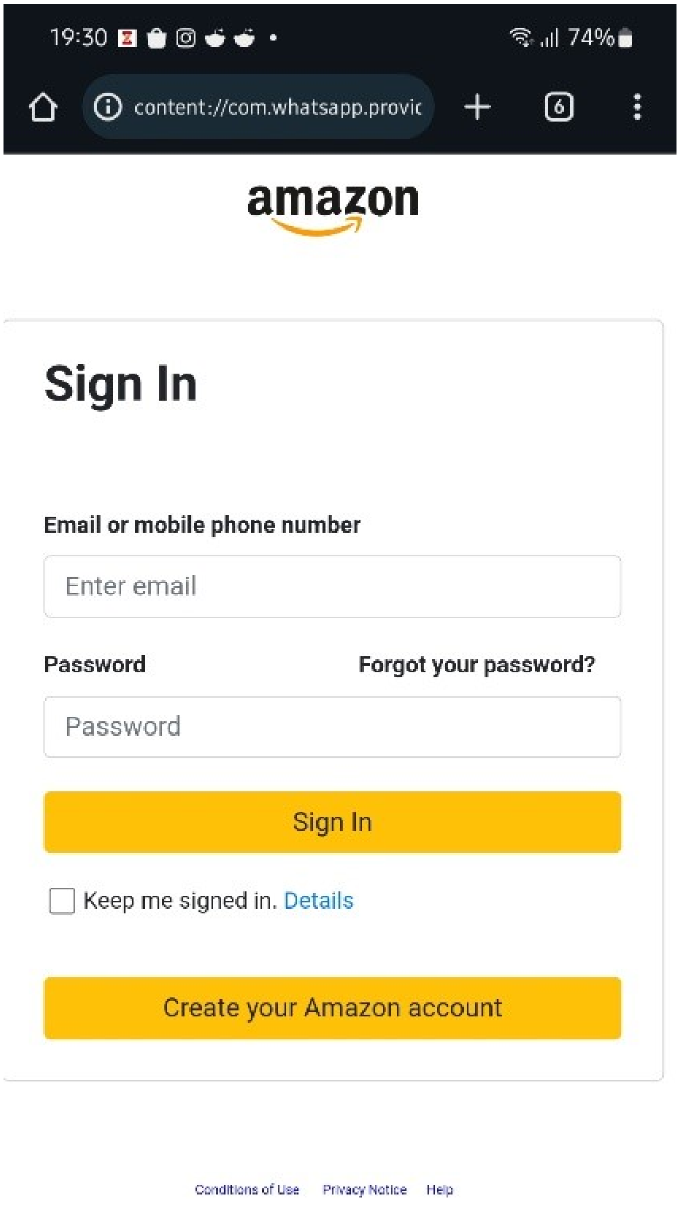
□ Keep me signed in. Details

Create your Amazon account

Conditions of Use Privacy Notice Help

Figure 1: Amazon Desktop

For this prototype user study, we initially planned to use domain names for hosting the phishing websites. We purchased nine domains from Namecheap.com with names resembling legitimate sites, such as "amazonos.site," which closely resembles "amazon.com." After purchasing these domains, we hosted our phishing websites on Google Cloud VM Instances using these domains. We even obtained SSL certificates for some of the websites to give them a more legitimate appearance. However, our account on Namecheap.com was suspended, and our hosted domains were taken down due to



19:30 74%

content://com.whatsapp.provic

amazon

Sign In

Email or mobile phone number

Enter email

Password Forgot your password?

Password

Sign In

□ Keep me signed in. Details

Create your Amazon account

Conditions of Use Privacy Notice Help

Figure 2: Amazon Mobile

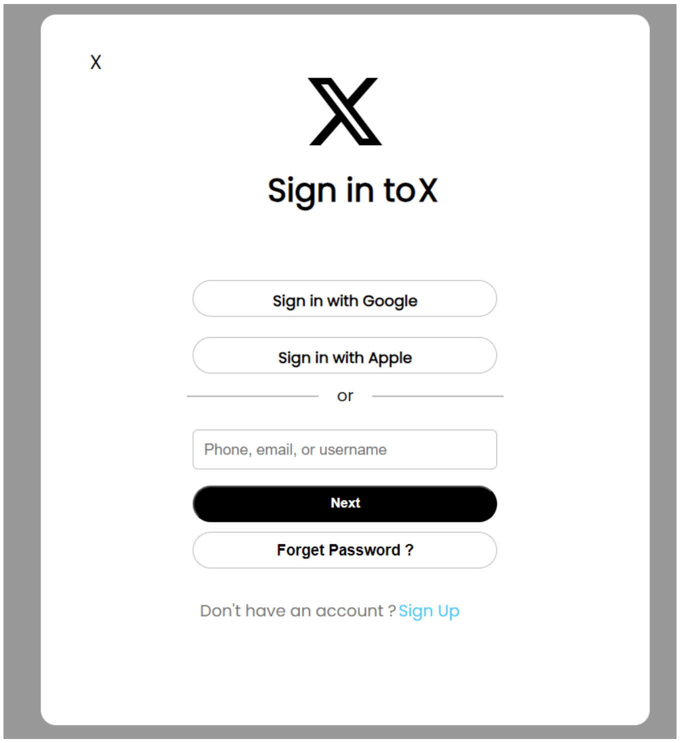


Figure 3: Twitter (X) on both platforms

legal concerns regarding malicious or phishing websites. Despite explaining that our sites did not collect any user data, our account remained suspended. As a result, we decided to host the websites directly on Google Cloud VM Instances without using a domain name. To mask the IP address URLs, we used URL shorteners like TinyURL and ShortURL. Participants in the study were informed to ignore the URL and focus only on the content of the website for this prototype study.

3.6.1 The Experiment Questionnaire. The following questions were asked for each website.

(1) Instructions: You will be provided a link to a website. Please visit the provided link then answer the questions based on your interaction with the link. Links clicked might open on the same tab, please navigate back to the survey after your visit to continue with the follow-up questions. Disclaimer: The website is hosted locally, hence the participant is requested to please ignore the URL and not consider it for this study.

(2) How would you rate the overall legitimacy and safety of the website you just visited?
   (a) Very Illegitimate
   (b) Somewhat Illegitimate
   (c) Neutral
   (d) Somewhat Legitimate
   (e) Very Legitimate

(3) How likely is this website high quality on each of these factors (asked separetely)? Website appearance, Website content, Spellings/Grammar, Overall
   (a) Poor
   (b) Below average
   (c) Average
   (d) Good
   (e) Excellent

(4) Based on your findings, what factors influenced your decision?
   (a) Appearance of the website
   (b) URL of the website
   (c) Content of the website
   (d) Presence of grammatical errors
   (e) Lack of 2FA (Two-Factor Authentication)
   (f) Absence of privacy policy or terms of service
   (g) Other ____________
   Please list any other reasons not mentioned above.

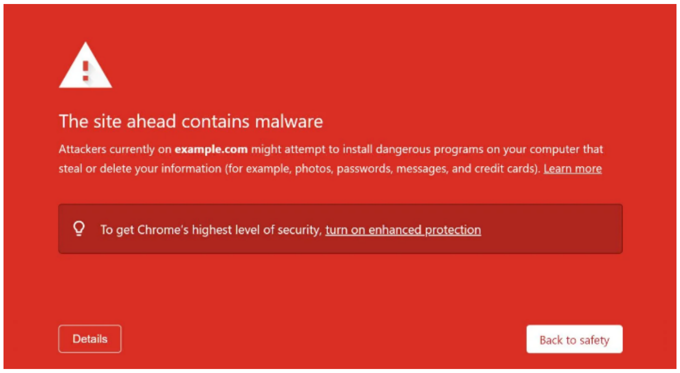
(5) Did you provide any sensitive information to the website?
   (a) Yes
   (b) No

3.7 Post Experiment Survey

We understand their thought process and determination techniques, like checking the website's appearance, the email, the URL, examining the content of the email and the website and finding any grammatical errors if any, fake forms and fields, lack of 2FA, no privacy policy or terms of service, and other factors for each participant. List all participant responses to the all websites, including whether they clicked on links, provided sensitive information, or reported it as not so high-quality website. We understand the knowledge gained by the participant after the whole experiment in-order to understand the spread of cyber security awareness.

3.7.1 Questions Asked.

(1) Are you aware of any Antivirus tools that prevent phishing scams on your system? If yes, which one:



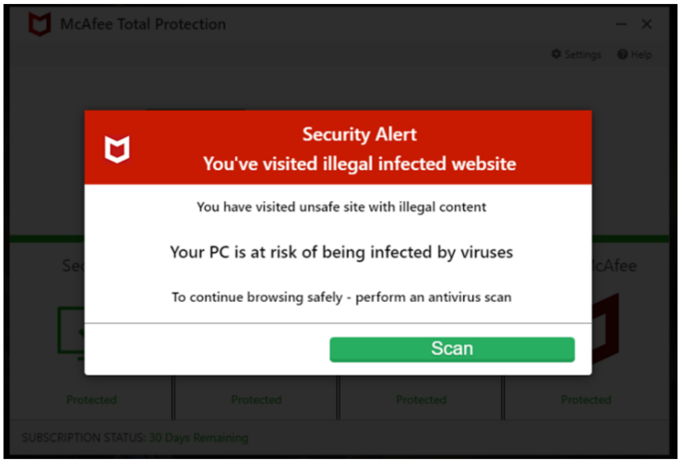
The site ahead contains malware

Attackers currently on **example.com** might attempt to install dangerous programs on your computer that steal or delete your information (for example, photos, passwords, messages, and credit cards). Learn more

To get Chrome's highest level of security, turn on enhanced protection

Figure 4: Google Safe Browsing

(2) Based on your experience, how well does your current Antivirus on your Web Browser in Desktop/Mobile platform perform?



Security Alert
You've visited illegal infected website

You have visited unsafe site with illegal content

Your PC is at risk of being infected by viruses

To continue browsing safely - perform an antivirus scan

SUBSCRIPTION STATUS: 30 Days Remaining

Figure 5: McAfee Total Protection

(a) Poor
(b) Below average
(c) Average
(d) Good
(e) Excellent

(3) Do you feel more aware of illegitimate sites and can you identify them after participating in this experiment?
(a) Yes
(b) No

(4) Would you change your behavior regarding clicking on links or providing information to websites after participating in this experiment?
(a) Yes
(b) No

(5) How likely are you to take proactive measures to protect yourself against cyber-attacks in the future?
(a) Very unlikely
(b) Unlikely
(c) Neutral
(d) Likely
(e) Very likely

(6) Any additional comments or feedback regarding your experience with the experiment in general? Comments/Suggestions:

(7) Please add Comments/Suggestions on this experiment:

We sought feedback from participants in this prototype experiment to identify areas where we could improve. This feedback is crucial for conducting a larger survey and the actual experiment.

4 RESULTS

The following results show demographics of the participants. Total participants for desktop is 5 and total participants for mobile is 6. Despite being a small sample, the demographics vary a lot. The above table 6 shows feature-wise percentage of how illegitimate the participants found it. After analysing the responses of all the features of each website, the participant legitimacy meter for each of the website is concluded as:

(1) Amazon_Illegitimate : 1 out of 5 thinks legitimate

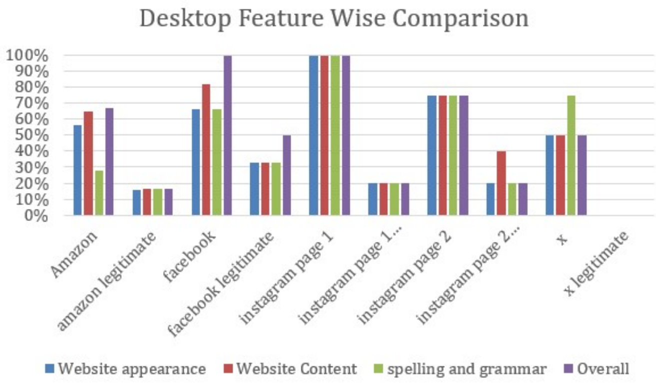


Figure 6: Desktop Illegitimacy Feature Wise Comparison

(2) Amazon_Legitimate : All think legitimate
(3) Facebook_Illegitimate : Mostly Neutral
(4) Facebook_Legitimate : Mostly illegitimate and Neutral
(5) Instagram page 1_Illegitimate: Illegitmate
(6) Instagram page 1_Legitimate: Legitimate
(7) Instagram page 2_Illegitimate: 1 out of 5 thinks legitimate
(8) Instagram page 2_Legitimate: Legitimate
(9) X_Illegitmate:Illegitmate
(10) x_Legitimate:Legitimate

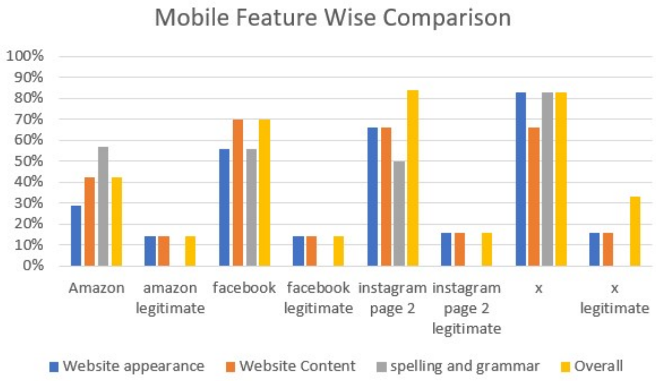


Figure 7: Mobile Illegitimacy Feature Wise Comparison

The above table 7 shows feature-wise percentage of how illegitimate the participants found it. After analysing the responses of all the features of each website, the participant legitimacy meter for each of the website is concluded as:

(1) Amazon_Illegitimate : 1 out of 6 thinks legitimate
(2) Amazon_Legitimate : All think legitimate
(3) Facebook_Illegitimate :2 out of 6 thinks legitimate
(4) Facebook_Legitimate : All think legitimate
(5) Instagram page 2_Illegitimate:3 out of 6 thinks legitimate
(6) Instagram page 2_Legitimate: Legitimate
(7) X_Illegitmate:1 out of 6 thinks legitimate
(8) x_Legitimate:Legitimate

Table 1: Participant Demographics

Age	Desktop (%)	Mobile (%)
25-34	54.55	40
18-24	9.09	60
35-44	36.36	-

Table 2: Race/Ethnicity

Race	Desktop (%)	Mobile (%)
Caucasian or White	63.64	-
Asian	36.36	90
Black or African American	-	10

Table 3: Education Qualification

Education	Desktop (%)	Mobile (%)
Doctoral Degree	54.55	-
Masters Degree	27.27	80
Bachelors Degree	18.18	20

Table 4: Gender

Gender	Desktop (%)	Mobile (%)
Male	45.45	100
Female	45.45	-
Prefer not to say	9.09	-

5 LIMITATIONS

While this study aimed to provide valuable insights into user behavior and susceptibility to phishing attacks, several limitations should be noted. Firstly, the sample size of participants may have been limited, primarily consisting of students from a single university. This may affect the generalizability of the findings to a broader population. Participants may have been more cautious or attentive during the study than they would be in their daily online activities, potentially influencing their responses and behavior. Furthermore, the study primarily focused on phishing attacks via email and may not encompass all forms of phishing attacks, such as SMS phishing (smishing) or voice phishing (vishing), which could present different behavioral patterns.Despite these limitations, the study provides valuable insights into phishing awareness and behavior, highlighting the need for further research in this area.

6 USER FEEDBACK

We received this feedback from the participants. The survey was informative, providing a good understanding of how to differentiate between fake and real websites based on visuals and other information. However, some questions lacked follow-up questions or had redundant options. For example, asking about antivirus tools without providing one if the answer is no. The experiment was considered good for improving awareness about phishing attacks and scams, showcasing variations between phishing and legitimate websites. Suggestions for improvement include adding more challenging and engaging questions, randomizing the website patterns, and including other types of scams like SMS spam or phishing emails for analysis.

7 CONCLUSION

Our Hypothesis is "Users are more likely to engage with phishing links when using mobile devices compared to desktop platforms".The hypothesis was confirmed, albeit with a narrow margin. The experimental results aligned with the initial hypothesis, indicating that the chosen approach was generally effective. However, the margin by which the hypothesis was supported was relatively small, suggesting that while the hypothesis holds true, there may be factors or nuances not fully accounted for in the experiment. This outcome underscores the need for further refinement and investigation to strengthen the hypothesis and its implications.

8 ACKNOWLEDGEMENT

We would like to acknowledge our Professor, Dr. Shirin Nilizadeh and our project mentor Mr. Sayak Saha Roy for their guidance and support while understanding and navigating through the challenges and problems faced in the project

REFERENCES

[1] Coopamootoo, K., and Gross, T. A systematic evaluation of evidence-based methods in cyber security user studies, 2019.

[2] Das, S., Kim, A., Tingle, Z., and Nippert-Eng, C. All about phishing: Exploring user research through a systematic literature review, 2019.

[3] Felt, A. P., and Wagner, D. Phishing on mobile devices.

[4] Heiding, F., Schneier, B., Vishwanath, A., Bernstein, J., and S. Park, P. Devising and detecting phishing: Large language models vs. smaller human models, 2023.

[5] Reinheimer, B., Aldag, L., Mayer, P., Mossano, M., Duezguen, R., Lofthouse, B., von Landesberger, T., and Volkamer, M. An investigation of phishing awareness and education over time: When and how to best remind users, 2020.

[6] Ribeiro, L., Guedes, I. S., and Cardoso, C. S. Which factors predict susceptibility to phishing? an empirical study. *Computers Security 136* (2024), 103558.

[7] Roy, S. S., Naragam, K., and Nilizadeh, S. Generating phishing attacks using chatgpt, 2023.

[8] Salem, M. B., and Stolfo, S. J. On the design and execution of cyber-security user studies: Methodology, challenges, and lessons learned, 2011.

[9] Shahriar, H., Klintic, T., and Clincy, V. Mobile phishing attacks and mitigation techniques. *Journal of Information Security 06*, 03 (2015), 206–212.

[10] Zhuo, S., Biddle, R., Betts, L., Arachchilage, N., Koh, Y., Lottridge, D., and Russello, G. What you see is not what you get: The role of email presentation in phishing susceptibility, 2023.