UNIVERSITY OF TEXAS ARLINGTON

INSTITUTIONAL REVIEW BOARD (IRB) FOR THE PROTECTION OF HUMAN SUBJECTS
APPLICATION FOR PRIMARY RESEARCH INVOLVING HUMAN SUBJECTS

UTA Faculty, staff, or students who propose to engage in any research, research development, testing or evaluation with human subjects must have review and approval from the UTA IRB prior to initiation. Some activities involving humans are not considered human subject research requiring IRB review (i.e., class projects, program evaluation, oral histories, quality improvement). Refer to the ***Research Project Chart*** *for more information.*

Utilize the* ***Required IRB Documents Chart *to guide you through the full IRB application process.* ***All study personnel must have completed Human Subjects Protection (HSP) Training prior to study approval. HSP Training expires and must be retaken every 3 years.*****

If you require assistance to complete this form or need additional information, please contact Regulatory Services at 817-272-3723 or regulatoryservices@uta.edu.

This version of the IRB Application Form should be used for ALL studies that will involve "*primary research*" with human subjects, defined as: the collection of new information or biospecimens from human subjects for research purposes by way of: 1) *interaction* with the individual, which includes any form of communication or interpersonal contact between the investigator(s) and the subject; and/or 2) *intervention* with the individual, which includes both physical procedures by which information or biological samples are gathered (like blood draws) and manipulations of the subject or the subject's environment for the research.

IMPORTANT: Studies that will involve only secondary research use of private identifiable information or identifiable biospecimens that have been (or will be) collected or generated for purposes other than the present research study should instead complete the UTA IRB Application for Secondary Research.

SECTION A: GENERAL INFORMATION

1. **Non-UTA Personnel:** *Enter all individuals that are* ***NOT affiliated with UTA*** *who will interact or intervene with human subjects for the research study OR who will access identifiable subject data.* ***UTA-affiliated*** *personnel should be listed on the electronic portion of the protocol (#3) in the electronic submission system.*

   ***Note:** In the electronic submission system, upload a completed Non-UTA Collaborator Form and Human Subject Protection training for each listed Non-UTA individual.*

Name:	Organization:

2. **Expected Start Date and Completion Date:** **04/12/24 – 04/19/24***(You are not authorized to start any research on human subjects including subject recruitment until the IRB has approved the research protocol.)*

3. **Funding:** *Indicate existing, potential, or pending sources of funding below (you may select more than one).*
   ***Note: If you do (or may) receive funding from NSF, NIH, CMMS, DOD, DOJ, DOE, DOEd, DOT, or any other federal agency, you MUST disclose this funding source below to ensure that your study is reviewed in accordance with the appropriate federal regulations for that specific federal funding source.**

   External:

   ☐ **Federal (Sponsor:)** ☐ **State (Sponsor:)** ☐ **Industry (Specify Sponsor:)**

   Grants & Contracts Bluesheet Number from Mentis:

Other:

☐ **UTA Department Account** ☐ **Personal Funds** ☐ **Other:** ☐ **None (*No funding*)**

SECTION B: RESEARCH CLASSIFICATION, RATIONALE, PROCEDURES, SITES, QUALIFICATIONS, OVERSIGHT

4. Research Classification: *Indicate if this study is categorized as* ***Minimal Risk (MR)*** *or* ***Greater than Minimal Risk (GMR).*** *"Minimal Risk (MR)" means that the probability and magnitude of harm or discomfort anticipated in the research are not greater in and of themselves than those ordinarily encountered in the subjects' daily life or during the performance of routine physical or psychological examinations or tests. "Greater than Minimal Risk (GMR)" refers to research activities that do not meet the definition of "Minimal Risk." Throughout this application form, there are additional questions or information requested for studies categorized as GMR; these instructions will be presented in purple.*

☒ **Minimal Risk (MR)** ☐ **Greater than Minimal Risk (GMR)**

***Note:** Studies that are federally funded and/or FDA regulated will be further classified into exempt, expedited, or full board in accordance with the Common Rule 45 CFR 46 and/or 21 CFR parts 50 and 56. See **Flowchart**.*

5. Rationale: *List the primary research questions, hypotheses, and / or objectives guiding this study.*

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?

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.

Hypothesis:

1. 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 click on phishing links.
    b. Users using mobile devices are more likely to submit credentials on phishing websites.
    c. Users using mobile devices are more likely to look for different features on phishing websites.

Expected Outcomes:

- Identification of differences in user behavior and susceptibility to phishing attacks on mobile devices versus desktops.
- Insights into user awareness and knowledge of phishing attack prevention on different platforms.
- Recommendations for improving cybersecurity awareness and resilience against phishing attacks.
    - The user study at the University of Texas at Arlington (UTA) is not only an opportunity to analyze user behavior and susceptibility to phishing attacks but also serves as a platform to educate participants about phishing attacks and spread awareness on cybersecurity. Participants, including students from different diversities and educational qualifications, will receive valuable information and insights into the tactics used by cyber attackers and how to protect themselves against such threats.
    - By the end of the experiment, participants will be better equipped to identify phishing attacks and take proactive measures to safeguard their personal and professional information. This initiative not only enhances cybersecurity awareness but also promotes a more secure and resilient campus community at UTA.

- We plan to inform participants at the end of the study about their performance, highlighting what they got right and where they may have missed certain phishing indicators. This feedback will help educate participants on how to identify phishing attacks more effectively in the future.

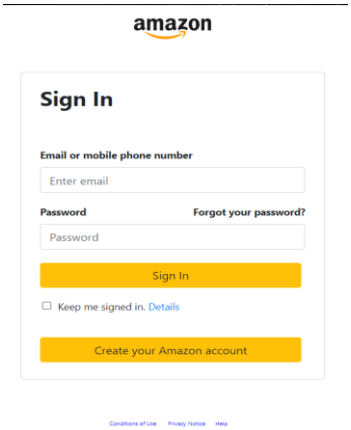
6. Procedures: *Describe the procedures step-by-step, including details on all methods that will be used to collect human subject data from the beginning to the end of the study. Describe what data will be collected (and if it will be individually identifiable); when and where the data will be collected; and how it will be collected (instruments or other measures). Use clear, concise layman's language that can be easily understood by persons outside your field and provide definitions for any technical terms. Add pictures if needed. If applicable, description and source of secondary research use of information and/or specimens.* ****Note: Refer to the Types of Research guidance page for a list of specific information required for different types of research.*** *For GMR research, it is also helpful to provide references or pilot data to support the proposed procedures.*

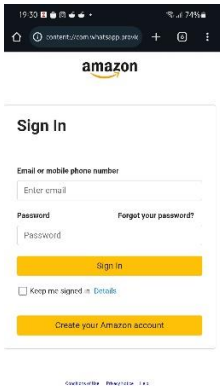
The experiment is split into 3 sections – pre-experiment survey, phishing attack simulation and post-experiment survey

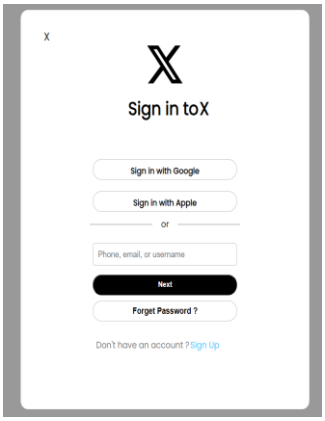
Pre -experiment survey – gather user demographics and knowledge on cyber security. Basic cyber security knowledge is asked to determine the level of knowledge the participants have on cyber security. Additionally, the participants are asked to rate themselves on how knowledgeable they think they are. This can be used to draw a contrast on the false sense of knowledge they pretend on having.

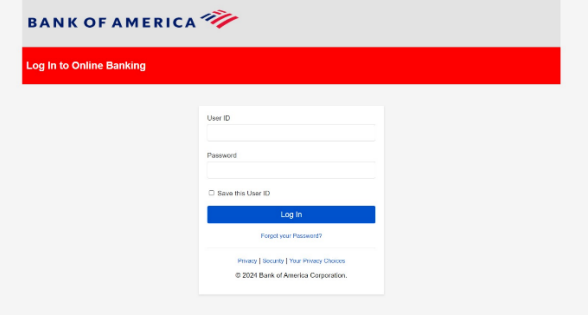
Phishing attack simulation – after we split the users in two for the two devices, participants undergo Identification/distinguishment of high quality and not so high-quality websites. The user goes through all links provided and rate each website if it is high quality. The user will be provided with 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), Bank of America. Screenshots of web 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, generative AI like ChatGPT and other sources like codepen.io, geeks for geeks, GitHub. This is done to simulate the real-world attacks.









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.

Duration: *Indicate how many participation sessions, interactions, or follow ups are expected for each subject participant, including the amount of time required for each visit and how long their total participation is expected to take (weeks, months, years, etc.) over the entire duration of the study. Please ensure that the duration described here is consistent with procedures and time-frames described elsewhere in the protocol application.*

Total duration of the experiment is 10 to 15 minutes for each participant with the estimated duration for each of the section as follows:

1. Pre-survey- 4 mins
2. Duration of experiment- 8mins
3. Post-survey- 4 mins

7. Alternatives to Participation: *Describe subjects' available options if they choose not to participate in the research study and clarify whether individuals that decline participation will still be subjected to the intervention (even if their data will not be utilized for research purposes). If research involves students, describe their alternatives to obtain course / extra credit if applicable. If research involves a health intervention, clarify whether individuals that decline will continue to receive standard care.*

The participant's participation in this study is voluntary, and they have the right to withdraw at any time without penalty. The data of the participant who have chosen not to participate will not be considered for the experiment.

8. Location(s) and Site(s): *Specify all locations where research procedures are expected to take place and which study procedures will take place at each site. Studies that take place online should specify the websites where data will be collected. Describe if any of the research will take place internationally. For multi-site research studies, review the web page for Collaborative Research. If any part of this study will be conducted in an institution or location administratively separate from UTA, indicate the institution(s) and upload a site permission letter.*

9. Personnel Qualifications: *List each member of the research team/personnel in the table below and describe 1) their role in the study, and 2) their relevant qualifications, special training, and experience as it pertains to the specific procedures or population of the study. If personnel will receive special training for conducting this study, please describe. If one or more personnel do not have any relevant qualifications or experience, please state that; the IRB will consider the risk level of the study and evaluate if additional oversight or input is necessary.*

Name of Research Personnel	Role in the study	Relevant qualifications, special training, and experience

Venkata Subrahmanya Abhinav Rallapalli	Researcher	Completed HSP training.
Vishal Reddy Vancha	Researcher	Completed HSP training.
Sivani Tumuluri	Researcher	Completed HSP training.

10. **Study Oversight:** *The Principal Investigator has ultimate responsibility for the conduct of this research, protection of subjects, and supervision of all protocol personnel. Describe your plan for oversight and communication to ensure that the entire research team: conducts the research ethically and in accordance with the approved protocol, creates/maintains appropriate study documentation and research records, and protects confidentiality of data. Your plan should address how the PI responsibilities are met. If a Faculty Advisor is overseeing student PI human subject research, the plan should address how the Faculty Advisor responsibilities are met.*

SECTION C: POPULATION & ENROLLMENT

11. **Population(s):** *Describe the target population(s) of the study, for example: UTA students, competent or healthy adults, children, prisoners, non-English speaking, pregnant women, individuals with impaired decision-making capacity, other vulnerable populations.*

- Recruit participants from diverse backgrounds, including different demographics (age, gender, occupation) and levels of cybersecurity awareness through email. Expected number of participants: 60.
- Participants are awarded a prize of $1 for participating in the study.
- Participants are primarily the students in UTA. Participants are recruited through email services. A participant receives an email with the consent form and providing them with the link of question pro platform on which the whole experiment is hosted.
- Participants are split into two groups – participants for mobile devices and desktop platforms. Participants are provided user credentials for the experiment. This way, no data of the participants is collected or used.
- Ensuring a sufficient sample size to ensure the study's validity and representativeness. Participants are split equally, that is, 30 participants for mobile platforms and 30 for desktop platforms. For both mobile and desktop platforms, the participant simply goes through the question pro survey.

Note: Additional forms may be required for your population. Obtain these from the Forms & Templates Page.

For Individuals with Impaired Decision-Making Capacity: Upload Form 2A.
For Pregnant Women, Fetuses, Women Undergoing In-Vitro Fertilization, or newborns: Upload Form 2B.
For Prisoners (Individuals involuntarily detained): Upload Form 2C.
For Children (Under 18 or the local legal adult age): Upload Form 2D.

12. **Inclusion Criteria:** *List all criteria for including subjects and explain the methods you will use to determine whether a subject is eligible based on your criteria (i.e., pre-screen, medical chart review). If your study is/will be funded, ensure that the inclusion criteria listed here match the details in your proposal.*

13. **Exclusion Criteria:** *Explain any specific factors or contraindications that would make a subject ineligible to participate in this study, even if they would otherwise meet the inclusion criteria listed above. Describe how the exclusion criteria will be verified. If your study is/will be funded, ensure that the exclusion criteria listed here match the details in your proposal.*

14. **Number of Subjects:** *Provide the number of subjects (or subject records/data sets) you intend to enroll over the course of the study. This information will be utilized by the IRB to understand the scope and logistics of the study; you*

may provide a projected range. For secondary research, please describe the number of records to be accessed.
60

***Note:** For MR research, after the protocol is approved, enrollment can exceed the number provided here without submitting a modification to the protocol.*

For GMR research, the proposed number of subjects must be supported by statistical justification and/or references; please provide that information here. Enrollment for GMR research is capped (IRB will approve a specific range or maximum number of participants and enrollment must not exceed that approved number unless the IRB approves a modification request).

15. **Recruitment Strategies:** *The first contact with a research participant is considered the beginning of research procedures, therefore describe how you will identify and contact potential participants, and how you will obtain their contact information. List who will provide access to contact information. Upload permission letters/emails as needed from individuals or organizations providing access to private contact information. Describe all your recruitment sources and methods.*

Participants are primarily recruited through email explaining them about the study and if they could volunteer participation. They would be informed briefly on what the experiment is, how is it conducted and how it will benefit them by increasing their cyber security awareness. The participant will be informed the total duration of the experiment.

16.a. Recruitment language and/or materials: *Provide the planned wording or language used in recruitment materials or scripts. Alternatively, upload a copy of all planned recruitment materials in the protocol submission. Examples include: letters/emails; website/social media posts; printed flyers; telephone scripts; subject pool posts (SONA, Mechanical Turk, Research Match); scripts for recruitment in-person.*

Sample email:

Subject: Invitation to Participate in Cyber Security Awareness Study

Dear potential participant,

We are conducting a study on cyber security awareness and would like to invite you to participate. Your participation in this study will not only contribute to valuable research but also increase your awareness of cyber security threats and how to protect yourself against them.
The study involves assessing multiple websites and categorizing them as high quality or not high-quality websites. Your actions and responses will help us understand user behavior and susceptibility to identification of high quality and not high-quality websites on mobile devices and desktops. The study takes 10-15 minutes to complete.
Participating in this study will provide cyber security awareness, which can help you protect yourself and others against online threats. Your participation is voluntary, and all information collected will be kept confidential and used for research purposes only.
If you are interested in participating or would like more information, please respond to this email or contact us at the provided researcher information below. We appreciate your time and consideration.
Sincerely,
Venkata Subrahmanya Abhinav Rallapalli
sxr8961@mavs.uta.edu

SECTION D: INFORMED CONSENT

***Note:** The ethical foundation of human subject research is informed consent. It is important to ensure that subjects are provided with sufficient information to understand the requirements of their participation and the use/purpose of their data. You also cannot obtain information about a person through another individual (such as a family member) unless that person has undergone the informed consent process themselves. Use the*

Office of Human Research Protection (OHRP) informed consent checklist (http://www.hhs.gov/ohrp/policy/consentckls.html) and the IRB's Templates as guidance.

16. **Informed Consent, Broad Consent, & Assent:** *Describe the informed consent process, including when, where, and how subjects will be consented. If children or mentally disabled or incapacitated persons will be subjects, explain the assent process. If broad consent (consent to use data for future studies) will be requested, describe the scope and the process for tracking subjects' accept/decline responses. Upload finalized copies of all consent, assent, and / or verbal consent script documents in the electronic system. If applicable, please address informed consent for any secondary research.* ***There are several consent form templates available for your use on the Forms & Templates Page.***

The participant is given an consent form to sign before the start of the experiment.

Consent/Disclosure Form:

Title: Cyber Security Awareness Study Consent/Disclosure Form

Introduction:

Thank you for participating in our study on cyber security awareness experiment. Before you proceed, please read the following information carefully.

Purpose of the Study:

The purpose of this study is to understand user behavior and susceptibility to identifying high quality websites on mobile devices and desktops. We aim to gather insights into how different demographics influence susceptibility to identifying such websites and how education and awareness impact behavior. Your participation will help us improve cybersecurity awareness and develop better strategies to protect against cyber security attacks.

About Cyber security attacks:

A cyberattack is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization. Example of such attacks are Denial of Service, Phishing, SQL injection, Ransomware, Trojan horse attack etc. Phishing is a form of social engineering and scam where attackers deceive people 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 few demographic questions along with general questions on cyber security awareness in the pre-experiment survey. This is to determine your cyber security knowledge. 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 if it is high quality or not so high quality. Some websites provided might be not 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. All credentials for all the websites used in the experiment will be provided by the researchers and NO actual user credentials are being used or collected. You are then requested to answer few post-experiment questions which discusses 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, including whether you clicked on the link, provided sensitive information (user credentials), or reported the website for not being high quality. 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. collected will be used to generalize and group participants to observe similarities between them. The responses to the websites including clicking on

the link, reason for clicking, providing sensitive information (user credentials), and reporting the website are used to perform quantitative analysis and understand similar behavior patterns.
Confidentiality and Participant rights:
Your participation in this study is voluntary, and you have the right to withdraw at any time without penalty. Your responses will be kept confidential, and your identity will not be linked to your data in any way. Only the research team will have access to the data, and all data will be stored securely.
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) giving 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

Participant Signature:

_____
(Signature)

Date:

_____

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

17a. Requesting a Waiver of Consent or Waiver of Written Documentation: *If you wish to waive some or all of the requirements of informed consent, or the requirement for written/signed informed consent, please describe (if your study is federally funded or FDA-regulated, also upload Form 3 from the Forms Page).*

17. Incomplete Disclosure / Deception: *Describe if your study will withhold information (incomplete disclosure) from subjects or involve deception regarding the purpose of the research or the nature of the intervention, interaction, or procedures. Provide scientific justification for utilizing incomplete disclosure or deception (if your study is federally funded, also upload Form 3.*

***Note:** "Incomplete disclosure" occurs when an investigator withholds information about the specific purpose, nature, or other aspect of the research. "Deception" occurs when an investigator gives false information to subjects or intentionally misleads them about some key aspect of the research.*

SECTION E: COMPENSATION AND COSTS

***Note:** You are responsible for maintaining accurate and confidential records regarding payment of your subjects. Per Accounting Services procedures, compensation must be documented for tax purposes using a W-9 form unless an exception is granted by the Accounting department. Obtaining an exception should be considered for cases of sensitive research or when disclosure of a subject's identity would expose them to high risk. Exception requests are submitted through the Business Affairs Exceptions Tracker (BAET) in SharePoint. Contact Business Technology Services at 817-272-2155.*

18. **Compensation:** *Describe any compensation to subjects for participation, including monetary payments, gift cards, course/extra credit, raffle prizes, goods or services, donations to charity, etc. Describe how and when you will provide the payment to the subjects, and how confidentiality will be maintained (for example, use of coding in payment logbooks/receipts). The IRB must understand how, when, and in what form you will be providing compensation. If compensation is pro-rated, please describe the pro-rate time points. If it's possible that a participant may be timed out, describe how this impacts compensation, if any. If you intend to hold a raffle, explain when you expect that the raffle will be drawn, and how participants will be contacted if they win the drawing. For course / extra credit, alternative non-research assignments must be offered for an equal amount of credit.*

Participants will receive $1 as a reward for participation.

Costs: *Describe any costs or expenses (monetary or non-monetary) subjects will incur as a result of participation.*

SECTION F: RISKS & BENEFITS

19. **Risks to Subjects:** *Explain any potential risks to subjects that could result from the research intervention/procedures, including **physical risks** (i.e. fainting, falls, infections, muscle soreness, pain, broken bones, physical fatigue, headache, burns, medication side effects); **psychological risks** (i.e. depression, anger, stress, guilt, embarrassment, damage to self-esteem); **social risks** (i.e. potential damage to financial standing, reputation, or employability); **risks to privacy or confidentiality** (i.e. exposing someone as a research subject, release or breach of sensitive data); and/or **risk of perceived coercion/undue influence** (i.e. if investigator could have influence by nature of their relationship or status, such as a teacher & student, manager & employee, doctor & patient).*

No risk to participants.

20. **Strategies to Minimize Risks:** *Explain the strategies that the research team will use to minimize <u>each</u> potential risk listed above.*

No personal identifiable information is collected. Collected data is stored in an anonymized format. All phishing sites are created by researchers and do not collect any data when clicked upon.

21. **Health & Safety Considerations:** *Specify whether the study involves any hazardous materials, locations, or equipment that is relevant to the health and safety of either the subjects or the protocol personnel (i.e. handling of human blood/body fluid/tissue, chemical or biological hazards, radiation/X-rays, lasers, or carcinogens). List any related authorizations/approvals from the Environmental Health & Safety Office.*

22. **Benefits:** *List potential benefits that may accrue directly to the study subjects as a result of their participation, if any (other than compensation). Also describe the expected or potential benefits of this study to the field or society at large.*

- The user study at the University of Texas at Arlington (UTA) is not only an opportunity to analyze user behavior and susceptibility to phishing attacks but also serves as a platform to educate participants about phishing attacks and spread awareness on cybersecurity. Participants, including students from different diversities and educational qualifications, will receive valuable information and insights into the tactics used by cyber attackers and how to protect themselves against such threats.
- By the end of the experiment, participants will be better equipped to identify phishing attacks and take proactive measures to safeguard their personal and professional information. This initiative not only enhances cybersecurity awareness but also promotes a more secure and resilient campus community at UTA.
- We plan to inform participants at the end of the study about their performance, highlighting what they got right and where they may have missed certain phishing indicators. This feedback will help educate participants on how to identify phishing attacks more effectively in the future.

SECTION G: PRIVACY & CONFIDENTIALITY

23. Privacy: *How will the privacy of subjects be protected during the course of the study (privacy refers to controlling the environment and circumstances of interactions with subjects to prevent situations where they might be embarrassed, exposed, or stigmatized)?*

We Protect participant privacy and confidentiality by anonymizing data and adhering to data protection regulations. No personal information of the participants is collected.

24. Confidentiality & Data Security

26a. Confidentiality: E*xplain if the data collected (including biospecimens) will be anonymous, identifiable/coded, or de-identified*. Explain the precautions that will be taken to protect confidentiality of subject data and information, and how these precautions will be communicated to subjects (during informed consent or another process).* ***NIH Studies:*** *Certificates of Confidentiality (CoCs) are automatically deemed to be issued for research that collects or uses identifiable, sensitive information. The informed consent template contains wording to inform research participants of this protection. If your study is subject to the NIH Data Management and Sharing (DMS) Policy, please be sure that the data types and controls defined in the approved plan are listed here.*

No personal identifiable data is collected from the participants. The collected experiment data is stored anonymously and the data is not shared with any third parties. Only the researchers have access to the data.

***Note:** "Anonymous" means that the data is unidentifiable (personally identifiable information will not be collected or accessed). "Identifiable" means that data obtained will be recorded in such a manner that subjects' identity can be readily ascertained, either directly or indirectly through identifiers linked to the subjects (research involving a coding mechanism that links to identifiable data is considered identifiable, but it is a helpful measure to protect confidentiality). "De-identified" means that all direct personal identifiers are permanently removed, no code or key exists to link the data to its original source, and the remaining information cannot reasonably be used by anyone to identify the source.*

26b. Data Security: *Security should be considered for each phase of data's life cycle, including collection, transmission, accessing, collaboration, storage, analysis, reporting, and disposition. Consider the tools and resources that will be utilized for data collection, how access to identifiable data will be limited only to authorized research personnel, and who will be responsible for storage and disposition.* ***Recordkeeping:*** *UTA and the IRB must be able to access research records and consent forms at any time; therefore,* ***all paper documents in their original form must be stored on the UTA campus*** *unless the IRB grants an exception.* ***All electronic data must be maintained on UTA servers utilizing sanctioned storage tools*** *unless the Office of Information Security grants an exception through the Technology Approval Process (TAP). Technology resources include software (both on your desktop and online), Software as a Service (SaaS) resources, apps, and related vendor services. Examples include project management software, simulation software, online criminal background check services, social media account management services, ticket sales services, mass email services, and online/electronic marketing services.* ***Record Retention Period:*** *All records (paper or electronic) must be maintained and kept secure for at least 3 years after the closure of the protocol or in accordance with funding agency requirements (whichever is longer). Student PIs should address long-term storage arrangements if planning to leave UTA prior to the end of the retention period.*

Visit the UTA IRB's Web Page on Human Subjects Data Security for allowable data storage options and more helpful information about DO's and DON'Ts with human subject data!

26c. Legal Limits to Confidentiality: *If any part of this study could result in the potential identification of child abuse, elderly abuse, communicable diseases, or criminal activities that would / could not have been otherwise identified, explain this possibility and estimate the likelihood of disclosure. Describe the plan of action that you will take if this occurs. In rare circumstances when research reveals these issues, confidentiality should be maintained to the extent that the law allows.*

25. **Data Sharing:** *If you intend to share, release, or present any identifiable subject data from this study, explain where, when, and to whom the identifiable information will be shared, presented or released, and how this will be communicated to the subjects beforehand.* ***NIH Studies****: If your study is subject to the NIH Data Management and Sharing (DMS) Policy, please be sure that the controls defined in the approved plan are listed here if the plan includes the sharing of identifiable data or de-identified data with controlled access.*

SECTION H: CONFLICT OF INTEREST

26. **Conflicts of Interest (COI):** *Does the principal investigator or any protocol personnel (internal and external) have an affiliation, arrangement, or financial interest that could be perceived as a conflict of interest? If yes, please describe. If the principal investigator or any protocol personnel (internal and external) have an active research conflict of interest management plan, please describe if the COI may be perceived as related to the research and provide a copy of the management plan.*

***Note**: "Financial Interest" is defined as anything of monetary value (existing or potential), whether or not the value is readily ascertainable. "Conflict of Interest" is defined as a significant financial interest that could directly and significantly affect the design, conduct, or reporting of research.*

***Note:** All Covered Individuals in GMR research are required to have a current COI disclosure on file in Mentis (this must be complete prior to approval of the protocol). Covered Individuals are those with responsibilities for the conduct, design, or reporting of this research study.*

SECTION I: REQUIRED ADDITIONAL ATTACHMENTS

27. **Upload finalized versions of the following documents as applicable to your study in the electronic submission system***:*

- Survey instruments / questionnaires (and any versions translated into other languages)
- Demographics surveys
- Interview questions / prompts
- Focus group instructions / questions / prompts
- Observation data collection sheets
- Psychological & educational tests
- Educational materials
- All recruitment materials including flyers, ads, scripts, emails, social media posts, etc.
- Informed Consent Documents / cover letters and translated versions (See Forms Page for Templates)
- Permission letters from non-UTA study sites / collaborating organizations
- Signed Non-UTA Collaborator Forms & HSP Training (Collaborative Research Page).
- Technology Approval Process Request Approval(s)