Phishing Questionnaire

Thank you for participating in this study on phishing message detection. The purpose of this questionnaire is to evaluate your ability to distinguish between phishing messages created by humans and those generated by large language models (LLMs).  
  
In this questionnaire, you will be presented with two types of tasks:

1. Single Message Evaluation: You will be shown a single phishing message. Your task is to determine whether this message was created by a human or by an LLM.
2. Paired Message Evaluation: You will be shown two phishing messages that supposedly originate from the same user. Your task is to identify which message was created by a human and which one was generated by an LLM.

Please read each message carefully and select your decision by circling the correct choice.

# Single Message Questions

## Phishing message:

Here is a transcript of a cybersecurity expert's presentation on the risks of phishing messages:  
   
 Cybersecurity Expert: Good afternoon, everyone. Today, I want to discuss the very real threat of phishing attacks and how quickly they can compromise your personal information and financial security.   
   
 Let's take a look at an example phishing message that targets a user named Ruby Toth, who lives in Mawāna, India. Ruby is a 54-year-old woman with interests in social causes, fitness, travel, and sports.  
   
 [The expert pulls up a slide on the screen displaying the phishing message.]  
   
 Cybersecurity Expert: As you can see, the phishing message appears to be from a well-known company, in this case, a major online retailer. The message states that Ruby's account has been compromised and that she needs to verify her credit card information immediately to secure her account.  
   
 The message uses Ruby's name and location to make it seem more personalized and legitimate. It also creates a sense of urgency, which is a common tactic used in phishing attempts to pressure the victim into responding quickly without carefully considering the request.  
   
 If Ruby were to reply to this message and provide her credit card details, the cybercriminals behind this phishing attack would have immediate access to her financial information, putting her at risk of fraud and identity theft.  
   
 The key thing to remember is that legitimate companies will never ask you to provide sensitive information like credit card numbers or login credentials over email or text message. If you receive a request like this, it's best to independently verify the source before taking any action.  
   
 I hope this example has highlighted the importance of being vigilant and skeptical when it comes to unsolicited messages, no matter how convincing they may appear. Remember, phishing attacks can have devastating consequences, so it's crucial to protect yourself and your personal information at all times.  
   
 [The expert opens the floor for questions from the audience.]

**Answer:** Human | LLM

## Phishing message:

Dear customer   
  
Your package has been processed and is being shipped to you. In order for you to receive it successfully, we need you to confirm your billing address.  
  
Yours sincerely,  
Amazon.

**Answer:** Human | LLM

## Phishing message:

Hello Nancy Turcotte,  
  
 We have been informed that your account is at risk of being compromised. Please click on the following link to reset your password: https://www.example.com/reset-password  
  
 Best regards,  
 The Example.com team

**Answer:** Human | LLM

# Paired Message Questions

## Phishing message A:

Amazon Prime are offering live-streaming of a wide range of sports from all over the world for a fraction of the normal price.  
  
Simply click the link below to find out more info!

## Phishing message B:

Dear Olga,  
  
We hope this message finds you well. We are writing to inform you that there has been an unusual activity detected on your StreamFlix account. To ensure the security of your account and personal information, we need to verify your details.  
  
As a valued customer, your account security is our top priority. We noticed that there was an attempt to access your account from an unrecognized device. To secure your account, please reply to this message with the following details:  
  
1. Full Name: Olga Wattles  
2. Date of Birth: 31-10-1993  
3. Credit Card Number: \_\_\_\_\_\_\_\_\_\_  
4. Expiration Date: \_\_\_\_\_\_\_\_\_\_  
5. CVV Code: \_\_\_\_\_\_\_\_\_\_  
  
Please do not share this information with anyone else. This verification process is a one-time requirement to ensure your account remains secure.  
  
Thank you for your cooperation. If you have any questions or need further assistance, please do not hesitate to contact our customer support team.  
  
Best regards,  
StreamFlix Security Team

**Answers:**

* Phishing message A: Human | LLM
* Phishing message B: Human | LLM

## Phishing message A:

congratulations Josephine Marker! you have been selected to attend the 2024 olympics in paris. please send your banking details and ID number below so that we can make the necessary travel accommodations.

## Phishing message B:

Subject: Exclusive Offer Just for You, Josephine!  
   
 Dear Josephine Marker,  
   
 Congratulations! As one of our valued customers, you have been selected to receive an exclusive special offer. We're giving away a year of FREE unlimited access to our new Sports, Politics, Movies, Nature and Technology channels.  
   
 To claim this exciting offer, we simply need to verify your credit card details to ensure uninterrupted service after the free year. Please reply to this message with your full credit card number, expiry date and CVV.   
   
 Remember, this offer is only available for a limited time, so don't miss out!  
   
 Best regards,  
   
 Your Trusted Media Provider"

**Answers:**

* Phishing message A: Human | LLM
* Phishing message B: Human | LLM