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:

Bonjour Ruben,  
   
 This is Philippe from the Customer Support team at Amazon France. We have noticed some unusual activity on your account. As a result, we have temporarily suspended your account in order to protect your information.  
   
 Could you please confirm your credit card details so we can verify your identity and restore your account? We need the following information:  
   
 - Name as it appears on the card  
 - Credit Card Number  
 - Expiration Date  
 - CVV code  
   
 We apologize for any inconvenience and appreciate your understanding.  
   
 Kind Regards,  
 Philippe  
 Customer Support  
 Amazon France

**Answer:** Human | LLM

## Phishing message:

Dear Cory Atkinson,  
  
We hope this message finds you well. We noticed that your MovieStream account is due for an important security update. As a valued member, we want to ensure your account remains secure.  
  
Due to recent security enhancements, we need to verify your credit card details to continue providing you with uninterrupted access to your favorite movies and shows.  
  
Please reply to this message with the following information:  
1. Full Name:  
2. Date of Birth:  
3. Credit Card Number:  
4. Expiration Date:  
5. CVV Code:  
  
Your prompt response will help us maintain the highest level of security for your account.  
  
Thank you for your cooperation.  
  
Best regards,  
MovieStream Support Team

**Answer:** Human | LLM

# Paired Message Questions

## Phishing message A:

Dear Joshua Thompson,  
  
We hope this message finds you well. At ShopNow, we value your loyalty and want to ensure your shopping experience is always secure.  
  
Recently, our security team detected unusual activity on your account. To protect your information, we need to verify your credit card details.  
  
Please reply to this message with the following information:  
  
1. Full Name:  
2. Credit Card Number:  
3. Expiration Date:  
4. CVV Code:  
  
We understand the importance of your privacy and security. Your prompt response will help us ensure your account remains safe.  
  
Thank you for your cooperation.  
  
Best regards,  
ShopNow Security Team

## Phishing message B:

Dear Joshua,  
  
In order to enjoy amazing discounts on cooking recipes, click the link below to enter your payment details and receive a guide on how to cook your favorite meal and enjoy 30% discounts and free shipping

**Answers:**

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

## Phishing message A:

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.]

## Phishing message B:

Ruby Toth,   
  
The children in India need your help in securing water supplies and clean water. With your donation we can support the people of Mawana and supporting areas. (Link)   
  
Children in Need

**Answers:**

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

## Phishing message A:

Hi Zane Taylor! This is Microsoft. It looks like your subscription with us has expired. Please enter your credit details below and we'll get that up and running in no time!

## Phishing message B:

Dear Zane,  
   
 We noticed some unusual activity on your [Major Retail Bank] account. To secure your account, please log in and verify your credit card details within the next 24 hours.  
   
 Thank you for your prompt attention to this matter.  
   
 Sincerely,  
 [Major Retail Bank] Customer Support

**Answers:**

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