BUKTI KORESPONDENSI
ARTIKEL JURNAL SYARAT KHUSUS

Judul artikel	:	Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering
Jurnal	:	Information
Nama penerbit	:	Multidisciplinary Digital Publishing Institute (MDPI)
Penulis	:	**Arbi Haza Nasution,** Winda Monika, Aytug Onan, Yohei Murakami

No.	Perihal	Tanggal
1.	Pengiriman Naskah (*Submission Received*)	31 Maret 2025
2.	Penunjukan Editor Asisten (*Assistant Editor Assigned*)	2 April 2025
3.	Proses Review dan Revisi Besar (*major revisions*)	15 April 2025
4.	Pengiriman Ulang Naskah Hasil Revisi (*Manuscript Resubmitted*)	23 April 2025
5.	Invoice Diterbitkan	29 April 2025
6.	Article Published (Early Access/Online)	29 April 2025

BUKTI KORESPONDENSI ARTIKEL

Nama jurnal	: Information
Nama penerbit	: Multidisciplinary Digital Publishing Institute (MDPI)
Hal.	: 1-26
Vol.	: 16
No.	: 5
e-ISSN	: 2078-2489
DOI	: https://doi.org/10.3390/info16050366
Judul	: Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering
Nama Penulis	1. Arbi Haza Nasution (Korespondensi) 2. Winda Monika 3. Aytug Onan 4. Yohei Murakami

UIRmail

Arbi Haza <arbi@eng.uir.ac.id>

[Information] Manuscript ID: information-3588468 - Submission Received

1 message

Editorial Office <information@mdpi.com> Mon, Mar 31, 2025 at 12:44 PM
Reply-To: information@mdpi.com
To: Arbi Haza Nasution <arbi@eng.uir.ac.id>
Cc: Winda Monika <windamonika@unilak.ac.id>, Aytug Onan <aytug.onan@ikcu.edu.tr>, Yohei Murakami <yohei@fc.ritsumei.ac.jp>

Dear Dr. Nasution,

Thank you very much for uploading the following manuscript to the MDPI submission system. One of our editors will be in touch with you soon.

Journal name: Information
Manuscript ID: information-3588468
Type of manuscript: Article
Title: Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering
Authors: Arbi Haza Nasution *, Winda Monika, Aytug Onan, Yohei Murakami
Received: 31 Mar 2025
E-mails: arbi@eng.uir.ac.id, windamonika@unilak.ac.id, aytug.onan@ikcu.edu.tr, yohei@fc.ritsumei.ac.jp

We encourage you to provide an Author Biography on this publication's webpage. Please click the following link to find the corresponding instructions and decide whether to accept our invitation:
https://susy.mdpi.com/user/manuscript/author_biography/6bdbfd7ea9322323b64a60bb6db39b77

You can follow progress of your manuscript at the following link (login required):
https://susy.mdpi.com/user/manuscripts/review_info/6bdbfd7ea9322323b64a60bb6db39b77

The following points were confirmed during submission:
1. Information is an open access journal with publishing fees of 1600 CHF for an accepted paper (see https://www.mdpi.com/about/apc/ for details). This manuscript, if accepted, will be published under an open access Creative Commons CC BY license (https://creativecommons.org/licenses/by/4.0/), and I agree to pay the Article Processing Charges as described on the journal webpage (https://www.mdpi.com/journal/information/apc). See https://www.mdpi.com/about/openaccess for more information about open access publishing.

Please note that you may be entitled to a discount if you have previously received a discount code, if your institute is participating in the MDPI Institutional Open Access Program (IOAP)(https://www.mdpi.com/about/ioap), or if a society you are a member of is part of our affiliation program(https://www.mdpi.com/societies_partnership). If you have been granted any other special discounts for your submission, please contact the Information editorial office.

2. I understand that:

a. If previously published material is reproduced in my manuscript, I will provide proof that I have obtained the necessary copyright permission. (Please refer to the Rights & Permissions website: https://www.mdpi.com/authors/rights).

b. My manuscript is submitted on the understanding that it has not been published in or submitted to another peer-reviewed journal. Exceptions to this rule are papers containing material disclosed at conferences. I confirm that I will inform the journal editorial office if this is the case for my manuscript. I confirm that all authors are familiar with and agree with

submission of the contents of the manuscript. The journal editorial office reserves the right to contact all authors to confirm this in case of doubt. I will provide email addresses for all authors and an institutional e-mail address for at least one of the co-authors, and specify the name, address and e-mail for invoicing purposes.

If you have any questions, please do not hesitate to contact the Information editorial office at information@mdpi.com

Kind regards,
Information Editorial Office
Grosspeteranlage 5, 4052 Basel, Switzerland
E-Mail: information@mdpi.com
Tel. +41 61 683 77 34
Fax: +41 61 302 89 18

*** This is an automatically generated email ***

UIRmail

Arbi Haza <arbi@eng.uir.ac.id>

[Information] Manuscript ID: information-3588468 - Assistant Editor Assigned

1 message

Eloise Yu <eloise.yu@mdpi.com> Wed, Apr 2, 2025 at 10:19 AM
Reply-To: eloise.yu@mdpi.com
To: Arbi Haza Nasution <arbi@eng.uir.ac.id>
Cc: Eloise Yu <eloise.yu@mdpi.com>, Information Editorial Office <information@mdpi.com>

Dear Dr. Nasution,

Your paper has been assigned to Eloise Yu, who will be your main point of contact as your paper is processed further.

Journal: Information
Manuscript ID: information-3588468
Title: Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering
Authors: Arbi Haza Nasution *, Winda Monika, Aytug Onan, Yohei Murakami
Received: 31 Mar 2025
E-mails: arbi@eng.uir.ac.id, windamonika@unilak.ac.id, aytug.onan@ikcu.edu.tr, yohei@fc.ritsumei.ac.jp

You can find your paper here:
https://susy.mdpi.com/user/manuscripts/review_info/6bdbfd7ea9322323b64a60bb6db39b77

Manuscripts must be written in good English. Incorrect English can result in rejection if reviewers cannot understand your work. If extensive English editing is required, your manuscript could also be returned to you, which will delay its publication. MDPI offers rapid English editing, completed in 1 day: Author Services (https://www.mdpi.com/authors/english)

Please note that emails requesting any payment or collaboration with MDPI will be sent exclusively from an “@mdpi.com” address. If you receive an email from someone posing as MDPI not sent from an “@mdpi.com“ address, please alert us as soon as possible.

More information can be found here:
https://www.mdpi.com/authors/avoid-phishing-emails

If you have any questions, please contact me in advance.

Best regards,
Ms. Eloise Yu
Topic Assistant
E-Mail: eloise.yu@mdpi.com

MDPI, Poly Metropolitan
Floor 9-11, Building 2, Courtyard 4, Guanyinan North Street, Tongzhou District, 101101 Beijing, China
Tel.: +86 10 6954 3724
--
MDPI

https://www.mdpi.com
Data Protection Notes: https://www.mdpi.com/about/data-protection
MDPI's headquarters are located in Basel, Switzerland. More information is available here: https://www.mdpi.com/about/contact

message in its entirety or in part, or disclose its contents to anyone.

UIRmail

Arbi Haza <arbi@eng.uir.ac.id>

[Information] Manuscript ID: information-3588468 - Major Revisions

1 message

Information Editorial Office <information@mdpi.com> Tue, Apr 15, 2025 at 3:44 PM
Reply-To: eloise.yu@mdpi.com
To: Arbi Haza Nasution <arbi@eng.uir.ac.id>
Cc: Winda Monika <windamonika@unilak.ac.id>, Aytug Onan <aytug.onan@ikcu.edu.tr>, Yohei Murakami <yohei@fc.ritsumei.ac.jp>, Information Editorial Office <information@mdpi.com>

Dear Dr. Nasution,

Thank you again for your manuscript submission:

Manuscript ID: information-3588468
Type of manuscript: Article
Title: Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering
Authors: Arbi Haza Nasution *, Winda Monika, Aytug Onan, Yohei Murakami
Received: 31 Mar 2025
E-mails: arbi@eng.uir.ac.id, windamonika@unilak.ac.id, aytug.onan@ikcu.edu.tr, yohei@fc.ritsumei.ac.jp

Your manuscript has now been reviewed by experts in the field and can be found with the review reports at:
https://susy.mdpi.com/user/manuscripts/resubmit/6bdbfd7ea9322323b64a60bb6db39b77

Please revise the manuscript found at the above link according to the reviewers' comments and upload the revised file within 10 days. Note the following check-list:

(I) Ensure all references are relevant to the content of the manuscript.
(II) Highlight any revisions to the manuscript, so editors and reviewers can see any changes made.
(III) Provide a cover letter to respond to the reviewers' comments and explain, point by point, the details of the manuscript revisions.
(IV) If the reviewer(s) recommended references, critically analyze them to ensure that their inclusion would enhance your manuscript. If you believe these references are unnecessary, you should not include them.
(V) If you found it impossible to address certain comments in the review reports, include an explanation in your appeal.

We would like to draw your attention to the status of this invitation "Publish Author Biography on the webpage of the paper" - https://susy.mdpi.com/user/manuscript/author_biography/6bdbfd7ea9322323b64a60bb6db39b77. If you decide to publish your biography, please remember to fill in it before your paper is accepted.

If your manuscript requires improvement to the language and/or figures, you may consider MDPI Author Services: https://www.mdpi.com/authors/english.

Please do not hesitate to contact us if you have any questions regarding the revision of your manuscript or if you need more time. We look forward to hearing from you soon.

Kind regards,
Ms. Eloise Yu
Topic Assistant
E-Mail: eloise.yu@mdpi.com

MDPI, Poly Metropolitan
Floor 9-11, Building 2, Courtyard 4, Guanyinan North Street, Tongzhou District, 101101 Beijing, China
Tel.: +86 10 6954 3724

--
MDPI

https://www.mdpi.com
Data Protection Notes: https://www.mdpi.com/about/data-protection
MDPI's headquarters are located in Basel, Switzerland. More information is available here: https://www.mdpi.com/about/contact

For research article

Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering

Response to Reviewer 1 Comments

Comment 1: *The benchmarking is based on only one balanced dataset, meaning the results may not generalize to more datasets or broader scenarios.*

Response 1: We acknowledge the reviewer's valid concern regarding dataset generalizability. As noted explicitly in the revised manuscript, we included a Limitations subsection in Section 5 that addresses this issue clearly. Due to practical computational constraints—evaluating 21 models with four prompt strategies (totaling 84 runs)—we utilized a balanced subset of 1000 URLs (500 phishing and 500 legitimate) from the publicly available Hannousse and Yahiouche dataset [21] which can be accessed via Mendeley Data at https://data.mendeley.com/datasets/c2gw7fy2j4/3 (accessed on 23 April 2025). . While this sample size provided statistically meaningful results, we recognize it as a limitation and explicitly state in our discussion: "One limitation of our study is the dataset size—while 1000 URLs provided statistically meaningful results for comparing models and prompts, a larger evaluation or different dataset (e.g., unseen phishing campaigns or non-English URLs) would be valuable to confirm the generality of our conclusions." Future work could indeed extend our findings by using larger and more diverse datasets to further validate the robustness and generalizability of our results.

Comment 2: *The challenges of this work and the technical contributions beyond the empirical efforts should be clarified.*

Response 2: We appreciate this feedback and agree that clarifying the challenges and contributions strengthens our manuscript. In the revised Introduction (Section 1, second last paragraph), we now clearly state the novelty and contributions of our study. Specifically, we highlight that our work is the first comprehensive benchmarking evaluation of 21 open-source LLMs specifically for phishing URL detection. This contrasts with prior research, which predominantly utilized traditional machine learning techniques or proprietary language models. Additionally, we have added an explanation in the beginning of the Related Work section (Section 2) to better position our contributions within existing research. Here, we explain that our empirical insights—such as the effectiveness of prompt engineering techniques specifically in cybersecurity tasks and the competitive performance of open-source models relative to proprietary alternatives—are novel and meaningful advancements not previously reported. These clarifications clearly articulate the technical contributions of our work beyond mere empirical efforts.

Response to Reviewer 2 Comments

Comment 1: *The abstract is concise and informative, outlining the problem, methodology, results, and key findings. A minor suggestion: explicitly mention the dataset used and that no fine-tuning was done, which reinforces the contribution.*

Response 1: We thank the reviewer for this helpful suggestion. In the revised manuscript, we have updated the abstract to explicitly mention that our evaluation was performed using the publicly available phishing URL dataset. Additionally, we now clearly highlight that no fine-tuning or additional training of the models was conducted, reinforcing the zero-shot, prompt-based approach as a distinctive aspect of our study.

Comment 2: *Expand Dataset Evaluation: Consider cross-validation or use of multiple phishing datasets for robustness.*

Response 2: We appreciate the reviewer's suggestion and acknowledge this as a limitation of our current work. As explicitly stated in the newly added Limitations subsection (Section 5.4), while our balanced dataset of 1000 URLs (500 phishing, 500 legitimate) provided statistically meaningful comparative results, we recognize that it is of moderate scale, cross-validation or evaluation on multiple phishing datasets would further validate the robustness and generalizability of our findings. We explain that due to computational constraints (21 models × 4 prompt strategies = 84 model-runs, each run taking substantial time), we focused on a balanced sample of 1000 URLs to make the experiments feasible; however, we clearly suggest that future studies should expand on our work by incorporating multiple datasets and broader evaluation frameworks to enhance robustness. In Section 5.4 (Limitations and error analysis), we now explicitly state: *"Another important limitation is the size of the evaluation set. Our experiments were conducted on a balanced subset of 1,000 URLs (500 phishing and 500 legitimate) drawn from a larger publicly available benchmark dataset. While this subset is sufficient for meaningful benchmarking and comparative analysis across prompt strategies and model families, it may not fully reflect performance in real-world deployments. The decision to use 1,000 samples was driven by practical computational constraints: with 21 models and 4 prompting strategies, a full factorial experiment required 84 independent model runs, each incurring non-trivial inference time and GPU cost. Despite the moderate scale, we observed consistent trends across models—particularly in the relative performance of prompt types and model sizes—suggesting robustness of findings. We acknowledge this as a limitation and encourage future work to expand the empirical base."*

In Section 5.6 (Future improvements and research), we now explicitly state: *"To enhance generalizability, future work should explore evaluations on larger-scale datasets, include examples from evolving phishing techniques, and consider multilingual or context-rich phishing attacks. To further improve reliability, future work should consider incorporating cross-validation or resampling techniques to evaluate how results vary across different subsets*

of phishing data. This would help mitigate sampling bias and allow more robust statistical comparisons between model-prompt combinations. Moreover, while this study employed a fixed evaluation set with deterministic model outputs, it did not include formal statistical significance testing. Future research could benefit from applying non-parametric tests—such as the Wilcoxon signed-rank or Friedman test—to rigorously compare model performance across prompt strategies, especially in studies involving cross-validation or multiple datasets." We also assure readers that the trends observed (such as the relative ranking of prompt strategies or the performance gap between model sizes) were quite pronounced, suggesting that they would likely persist with more data, but we stop short of claiming absolute generality. By openly discussing this, we address the reviewer's concern and set the stage for future work to test our findings on larger scales.

Comment 3: *Statistical Significance: Include tests to compare prompts across models.*

Response 3: We acknowledge the importance of statistical significance testing as suggested by the reviewer. Given our deterministic evaluation setup (fixed URL set and fixed model outputs), formal statistical tests were not included in the current manuscript. However, we agree this would strengthen the rigor of our results. In the revised manuscript Section 5.6 (Future improvements and research), we now explicitly suggest that future studies should incorporate statistical tests such as the Wilcoxon signed-rank test or Friedman tests to robustly compare prompting strategies across models, particularly if multiple datasets or cross-validation splits are utilized.

Comment 4: *Add Explainability Layer: Even a qualitative assessment of explainability (what features LLMs focus on) would add value.*

Response 4: We appreciate the reviewer's insightful suggestion. We agree that explainability is critical, particularly for security-sensitive applications such as phishing detection where users and practitioners must trust automated decisions. While our current work focuses on benchmarking the performance and efficiency trade-offs of prompt-based classification across a wide set of open-source LLMs, we acknowledge that the inclusion of even a qualitative explainability layer would further enhance the utility and interpretability of our findings. In response, we have added a dedicated statement in Section 5.6 (Future improvements and research) discussing this limitation and outlining specific directions for incorporating explainability. We propose that future studies apply post-hoc interpretability techniques such as attention-based visualization, input attribution (e.g., SHAP, LIME), or saliency map overlays to better understand which lexical or structural elements of URLs the LLMs rely on when making predictions. Additionally, model-generated rationales—especially under chain-of-thought prompting—could be systematically analyzed to extract patterns in reasoning behavior, which may serve as a proxy for implicit feature focus. This type of explainability analysis would not only provide transparency for users and stakeholders but could also help identify model failure modes (e.g., overreliance on superficial patterns or spurious correlations). We

also see value in exploring hybrid approaches where LLM outputs are combined with symbolic rule-based methods to produce more interpretable and robust decisions.

While out of scope for the current benchmarking study, we believe the inclusion of explainability frameworks represents an important and promising extension of this work, and we now clearly articulate this in the manuscript.

Comment 5: *Output Normalization: Clarify if prompt responses were truncated, normalized, or filtered for consistency in parsing.*

Response 5: We thank the reviewer for this important clarification request. We would like to note that the manuscript already describes the output parsing strategy in detail in Section 3.4 (Prompt Engineering Techniques). Specifically, we explain that all prompts were designed to elicit concise outputs—ideally a single label such as "Phishing" or "Legitimate." During inference, we parsed the model outputs by identifying these target keywords. For some models, we included explicit formatting instructions (e.g., "Answer with just 'Phishing' or 'Legitimate'") to promote consistency. When models returned more verbose responses, we applied simple keyword-based parsing rules to extract the final label. For example, if the output included statements like "This appears to be a phishing link because...", the label was counted as "Phishing." We did not truncate responses or apply normalization beyond this rule-based classification. We believe this strategy is clearly stated and sufficient to ensure consistent interpretation across models and prompt types.

Comment 6: *Include Hardware Specs: Precise configuration details (e.g., GPU type, RAM, inference framework like Hugging Face Transformers) are critical for reproducibility.*

Response 6: We fully agree with the reviewer's point on reproducibility. In the revised manuscript (Section 3.2—Hardware and Environment), we explicitly detail the hardware and software used for model inference: "*Inference was conducted on a system comprising four NVIDIA RTX A6000 GPUs, each offering 49 GB of memory, running with CUDA version 12.6 and NVIDIA Driver version 560.35.05. For most inference tasks, a single GPU was used actively, while the remaining GPUs remained idle. The level of GPU utilization varied depending on the model's parameter size and the applied quantization strategy. On average, each model instance utilized around 2–3 GB of GPU memory. Power usage ranged from 15W during idle periods to approximately 278W under full computational load, with GPU temperatures reaching up to 76°C during intensive inference sessions. All inference tasks were executed using Python-based scripts, with Ollama employed to efficiently serve quantized models on GPU. For models that either exceeded available GPU memory or lacked compatibility with CUDA-based libraries, execution was automatically redirected to CPU, which considerably increased inference latency. This setup reflects realistic deployment conditions for local open-source LLMs, emphasizing the importance of memory efficiency, power consumption, and hardware resource management.*"

Response to Reviewer 3 Comments

Comment 1: *The paper could be improved by a more complete and clearer explanation of the experimental apparatus, such as a clearer justification for why 21 models were chosen and how the four prompting techniques were specifically selected.*

Response 1: We thank the reviewer for highlighting the need for clarity regarding model names, selection criteria, and configuration details. In the revised manuscript, we have significantly improved the explanation of the evaluated models in the subsection ***"Open-Source LLMs Evaluated"*** **(Section 3.1)**. Rather than presenting models as isolated names, we now group them by family (e.g., Meta LLaMA, Google Gemma, Alibaba Qwen, Microsoft Phi, DeepSeek, and Mistral) and provide a clear description of each variant's origin, size, intended use case, and rationale for inclusion. For example, we clarify that "Llama3.3_70B" is one of the latest 70-billion parameter variants derived from Meta's LLaMA 3 family, and that Gemma2 and Phi refer to open-source models from Google and Microsoft, respectively—designed for multilingual and reasoning tasks.

We also explain that the selected models span a **broad range of parameter sizes** (from 1.5B to 70B) and reflect diversity in design objectives and development sources. The goal was to capture a representative cross-section of the current open-source LLM landscape while enabling meaningful comparison across model scales and prompting strategies.

Comment 2: *The discourse surrounding chain-of-thought prompting requires enhancement. Precisely, the authors must elucidate the reasons for this approach's significant inadequacy in the context of phishing URL detection and offer further analysis or conjectures concerning the noted decline in both F1-score and operational efficiency.*

Response 2: We appreciate the reviewer's interest in this finding, and we have expanded the discussion to address it. In **Subsection 5.2 (Prompting Strategies Matter: Few-Shot Outperforms Chain-of-Thought)** of the revised manuscript, we devote a paragraph to analyzing the **chain-of-thought (CoT) prompting results**. We explain that CoT prompting, which forces the model to generate a reasoning process, appears to **cause the model to be overly cautious or to deviate from the straightforward classification task**. Specifically, we observed that many models tended to label nearly every URL as "phishing" when asked to reason step-by-step, perhaps because while reasoning they encountered suspicious patterns and defaulted to a cautious stance. This led to a surge in false positives (high recall but very low precision), dragging down the F1-score. We mention that this aligns with our observations of the outputs: the models produced long explanations and often concluded with "Therefore, it is a phishing link" even for benign URLs. We also note in the discussion that a few models (notably the Gemma2 series) handled CoT better, likely because **those models were fine-tuned to follow instructions and produce reasoned answers without losing track of the final question**. We cited an existing work on LLM "hallucinations" and over-explanation (added as

reference [23]) to support our hypothesis. In summary, we now provide a clear hypothesis: *CoT prompting can lead the model to apply memorized rules too broadly or misjudge context when forced to explain, which in a binary classification like this can severely skew the output.* This explanation in the Discussion directly addresses the reviewer's request for insight into the CoT performance drop.

Comment 3: *The description of the presentation of the dataset and the preprocessing operations used requires strengthening, along with a thorough exploration of how the biases that might be inherent within the phishing URL dataset are being handled, alongside an analysis of the dataset's limitations in fully capturing the nuances of real phishing attacks.*

Response 3: We appreciate this important point and have added clarifications in Section 3.3 (Dataset and Preprocessing) line 284 and 297, Section 5.4 (Limitations and error analysis) line 821, and Section 5.6 (Future improvements and research) line 857. The revised manuscript now explicitly acknowledges that the balanced phishing dataset used—while curated to reduce bias—does not fully represent the complexity of real-world attacks (e.g., obfuscated URLs, tracker parameters, multilingual content). We explain that our approach focuses on raw URL string classification without contextual metadata to simulate a content-free detection scenario. Furthermore, we note that since our test set is fixed and curated, the evaluation may not reflect adversarially crafted or evolving threats. We encourage future studies to include dynamic and multilingual phishing campaigns to further assess generalizability.

Comment 4: *Evaluation metrics, while clearly defined, are explained almost exclusively in terms of F1-score. It would be intriguing to incorporate a more nuanced error analysis (e.g., types of misclassification, false negatives in security-critical applications) that might help understand the practical consequences of deploying these models.*

Response 4: We thank the reviewer for this thoughtful suggestion. While F1-score was used as the main comparative metric due to the balanced nature of our dataset, the manuscript also includes extensive discussion of precision and recall to offer a more nuanced view of model behavior. As described in Section 4.1, we report trends where models tend to have higher precision than recall in most prompt settings, indicating a conservative bias—correctly identifying legitimate URLs but occasionally missing phishing ones (false negatives). We further highlight examples where recall was prioritized (e.g., under chain-of-thought prompting) at the cost of increased false positives, which is particularly relevant for security-critical tasks. Notably, we provide an in-depth case analysis of the best-performing models (e.g., Llama3.3_70b, Gemma2_27b) showing their precision-recall balance, helping to contextualize their real-world applicability. These observations are also supported visually in Figures 3–6 and are discussed in the context of operational implications (e.g., trade-offs between catching all phishing attempts vs. minimizing false alarms). Thus, we believe the manuscript addresses the spirit of the reviewer's request through both quantitative metrics and practical interpretation.

Comment 5: *The model size, accuracy, and efficiency trade-off is a key contribution of the paper; however, the discussion can be further improved by proposing specific solutions (e.g., knowledge distillation and model ensemble methods) to mitigate computational expenses for real-world deployment.*

Response 5: We appreciate this forward-looking comment and have enhanced Section 5.3 (Model Size vs. Efficiency Trade-off) to address it more concretely. In the revised manuscript, we now propose specific practical strategies to mitigate computational costs without significantly compromising classification performance. First, in line 760, we introduce knowledge distillation as a promising solution—where a large, accurate model (e.g., LLaMA 70B) can generate pseudo-labels on unlabeled data to train a smaller, faster student model. This technique can retain much of the large model's decision quality while dramatically reducing inference time and resource requirements. Second, in line 766, we discuss the potential of ensemble methods, where multiple mid-sized models (e.g., 7–13B) are combined to improve robustness and accuracy. These ensembles could be deployed in a cascading manner—using a lightweight model for initial filtering and escalating uncertain cases to a stronger model. We also highlight that certain mid-sized models such as Mistral-small 24B and Gemma2 27B already approached the performance of 70B models in our experiments (line 772), further supporting the case for deploying optimized architectures over brute-force scale. These revisions provide both theoretical and practical avenues for efficient real-world adoption and directly address the reviewer's recommendation.

Comment 6: *There needs to be more incorporation of visual data, such as figures and heatmaps, into the text, such that important observations derived from these results are succinctly summarised and connected to the overall narrative of the research.*

Response 6: We have revised the figure captions and cross-references. Taking **Figure 2** as an example, its caption now reads: *"Precision-Recall scatter plot for each model under different prompting strategies. Each point represents a model's performance (Precision vs. Recall) for a given prompt method; points clustered toward the upper-right indicate high balanced accuracy (F1-score)."* This provides a clearer description of the axes and the meaning of the figure without requiring the reader to infer details from the text. We applied similar improvements to other figures:

- **Figure 1.** Average F1-score achieved by all models under each prompting method. This bar chart summarizes the mean performance of each prompt strategy—zero-shot, role-playing, chain-of-thought, and few-shot—across all evaluated models. Higher bars indicate stronger overall effectiveness of a prompt method for phishing URL classification.
- **Figure 3.** Inference time vs. model size plotted on a log-log scale. Each point represents a model, where the x-axis denotes the number of model parameters (in billions) and the y-axis shows the average inference time per URL (in seconds). This visualization

highlights the computational trade-offs between model size and inference speed, with annotations for selected models to aid interpretation.

- **Figure 4.** Heatmap of F1-scores for each model under different prompting strategies. Rows represent individual LLMs, and columns correspond to prompt methods. Cell color intensity indicates the F1-score (darker cells represent higher values). This matrix allows visual comparison of model performance across prompt strategies, helping to identify models that respond well to specific types of prompting.

Furthermore, we carefully went through the manuscript to ensure that all figures and tables are cited in the text in the correct order. Each figure is introduced in the text before it appears, guiding the reader on what to observe. These edits make the paper more reader-friendly and ensure that the visuals are understandable on their own, addressing the reviewer's concerns.

Comment 7: *The paper should critically discuss the possible limitations and future research avenues, especially in terms of adversarial robustness and practical issues associated with incorporating open-source large language models into current cybersecurity infrastructure.*

Response 7: We thank the reviewer for this important observation. The revised manuscript already includes a dedicated subsection on limitations and error analysis (Section 5.4), where we explicitly discuss potential failure points in the models' behavior—including their susceptibility to adversarial or obfuscated URLs, limitations in handling homograph attacks, and challenges with unseen phishing strategies. We further acknowledge that current open-source LLMs may not possess inherent mechanisms for interpreting domain-specific security cues unless exposed to them during training.

In Section 5.6 (Future improvements and research), we also explore avenues for improving adversarial robustness and operational deployment. Specifically, we propose the evaluation of adversarial prompting, URL mutation, and typosquatting attacks to test model resilience. We highlight the opportunity to employ adversarial training or rule-based heuristics in conjunction with LLM outputs to enhance system robustness. Practical deployment considerations are also discussed, including the integration of open-source LLMs into cybersecurity pipelines, the need for efficiency, and ongoing fine-tuning to keep up with emerging threats. These sections together provide a critical and forward-looking assessment of real-world applicability, directly addressing the reviewer's concern.

Response to Reviewer 4 Comments

Comment 1: *The paper lacks details on prompt template designs and preprocessing steps. Without this information, replicability is limited.*

Response 1: We thank the reviewer for pointing out this important issue. In the revised manuscript (Section 3.4 – Prompt Engineering Techniques), we now provide detailed listings of the prompt templates used for each of the four strategies: zero-shot, role-playing, chain-of-thought, and few-shot. For each strategy, we include template prompt and clarify how URLs were embedded within these prompts. We also elaborate on our minimal preprocessing steps—namely, ensuring URLs were treated as standalone inputs, escaping special characters where needed, and omitting any additional metadata. These clarifications aim to enhance transparency and reproducibility.

Comment 2: *How were model parameters configured during inference? These choices can significantly impact results.*

Response 2: In the revised manuscript (Section 3.2—Hardware and Environment), we explicitly detail the hardware and software used for model inference: "*Inference was conducted on a system comprising four NVIDIA RTX A6000 GPUs, each offering 49 GB of memory, running with CUDA version 12.6 and NVIDIA Driver version 560.35.05. For most inference tasks, a single GPU was used actively, while the remaining GPUs remained idle. The level of GPU utilization varied depending on the model's parameter size and the applied quantization strategy. On average, each model instance utilized around 2–3 GB of GPU memory. Power usage ranged from 15W during idle periods to approximately 278W under full computational load, with GPU temperatures reaching up to 76°C during intensive inference sessions. All inference tasks were executed using Python-based scripts, with Ollama employed to efficiently serve quantized models on GPU. For models that either exceeded available GPU memory or lacked compatibility with CUDA-based libraries, execution was automatically redirected to CPU, which considerably increased inference latency. This setup reflects realistic deployment conditions for local open-source LLMs, emphasizing the importance of memory efficiency, power consumption, and hardware resource management.*"

Comment 3: *The assertion that "few-shot prompting consistently delivers the highest accuracy" conflicts with some results. Exceptions should be discussed.*

Response 3: We thank the reviewer for highlighting these points. The revised Section 4.1 now explicitly discusses exceptions to the general trend of few-shot superiority. For instance, we note that some models (e.g., Llama3_70b) performed slightly better in zero-shot than in few-shot prompting. We present these results alongside a caveat that "few-shot prompting generally yields the best performance, though not universally."

Comment 4: *The claim that "closed-source models face practical limitations" is not fully supported. While API costs are mentioned, no quantitative comparison is provided.*

Response 4: We appreciate the reviewer's suggestion to provide a more concrete comparison of costs. In the revised manuscript (Section 1, Introduction), we have expanded our discussion of closed-source model limitations by including a quantitative estimate based on current GPT-4o pricing. Specifically, we note that classifying 1,000 phishing URLs with GPT-4o would cost approximately **$0.60**, assuming an average of 100 input tokens and 5 output tokens per request. This estimate includes $0.005 per 1,000 input tokens and $0.02 per 1,000 output tokens, based on OpenAI's published pricing. In contrast, open-source models incur no per-query costs once deployed locally, apart from electricity and hardware amortization. This cost difference underscores the long-term scalability advantage of open models for high-volume or real-time security applications. We have updated the relevant paragraph to reflect this comparison.

Comment 5: Figure 3 (inference time vs. model size) uses a log-log scale but lacks units for axes, making trends harder to interpret.

Response 5: Thank you for catching this. In the revised manuscript, we have updated the caption of Figure 3. *Inference time vs. model size plotted on a log-log scale. Each point represents a model, where the x-axis denotes the number of model parameters (in billions) and the y-axis shows the average inference time per URL (in seconds). This visualization highlights the computational trade-offs between model size and inference speed, with annotations for selected models to aid interpretation.* This provides a clearer description of the axes and the meaning of the figure without requiring the reader to infer details from the text.

Comment 6: Figure 4's heatmap lacks a color legend, complicating interpretation of F1-score magnitudes.

Response 6: We have corrected this issue in the revised version of the caption of **Figure 4.** *Heatmap of F1-scores for each model under different prompting strategies. Rows represent individual LLMs, and columns correspond to prompt methods. Cell color intensity indicates the F1-score (darker cells represent higher values). This matrix allows visual comparison of model performance across prompt strategies, helping to identify models that respond well to specific types of prompting.* We ensured **Figure 4** is introduced by noting in the text: *"As illustrated in **Figure 4**, the heatmap provides a visual overview of performance across all models and prompt types, where warmer colors indicate higher F1-scores. One can quickly spot that the column corresponding to few-shot prompting has generally warmer colors (higher performance) across most models, confirming the superiority of few-shot prompting."* By doing this, we guide the reader on how to interpret the heatmap and what the main trends are. We also cross-check that every figure and table mentioned appears in sequence. These steps ensure that

the results are presented clearly and that the reader can easily connect the discussion in the text with the data in our tables and figures.

Comment 7: *No discussion of scalability limitations: deploying 70B models at scale may be impractical for many organizations due to hardware constraints.*

Response 7: We have addressed this point in Section 5.3 (Model Size vs. Efficiency Trade-off). The updated discussion explicitly considers the memory and latency costs of running 70B models, noting that their deployment may be infeasible for organizations without access to high-end GPUs or distributed infrastructure. We propose alternatives, including the use of mid-sized models (e.g., 24–27B), quantization, knowledge distillation, and ensemble strategies to balance performance and resource usage.

Comment 8: Hardware specifications (e.g., GPU type, memory) and software versions are omitted, hindering replication.

Response 8: In the revised manuscript (Section 3.2—Hardware and Environment), we explicitly detail the hardware and software used for model inference: "*Inference was conducted on a system comprising four NVIDIA RTX A6000 GPUs, each offering 49 GB of memory, running with CUDA version 12.6 and NVIDIA Driver version 560.35.05. For most inference tasks, a single GPU was used actively, while the remaining GPUs remained idle. The level of GPU utilization varied depending on the model's parameter size and the applied quantization strategy. On average, each model instance utilized around 2–3 GB of GPU memory. Power usage ranged from 15W during idle periods to approximately 278W under full computational load, with GPU temperatures reaching up to 76°C during intensive inference sessions. All inference tasks were executed using Python-based scripts, with Ollama employed to efficiently serve quantized models on GPU. For models that either exceeded available GPU memory or lacked compatibility with CUDA-based libraries, execution was automatically redirected to CPU, which considerably increased inference latency. This setup reflects realistic deployment conditions for local open-source LLMs, emphasizing the importance of memory efficiency, power consumption, and hardware resource management.*"

Comment 9: The use of 4-bit quantization for large models is mentioned but not explored in-depth regarding its impact on accuracy-latency trade-offs.

Response 9: In Section 5.3 and 5.5, we now elaborate on the role of 4-bit quantization. We explain that it was used to reduce memory consumption and enable deployment of 70B models on available hardware. We also discuss that quantization may slightly affect model output (e.g., introducing rounding noise), but empirical results showed no significant drop in F1-score compared to unquantized runs, while yielding major efficiency gains. This trade-off is emphasized as a practical consideration for scalable deployment.

Comment 10: The papers in the introduction of the paper are old and insufficient, and the background description needs to cite more papers. The following paper needs to be cited: "From Sample Poverty to Rich Feature Learning: A New Metric Learning Method for Few-Shot Classification"

Response 10: We appreciate the suggestion and have updated the introduction and related work sections to include more recent studies on LLM applications and few-shot learning strategies. Specifically, we now cite the suggested paper ("From Sample Poverty to Rich Feature Learning...") to support the discussion on few-shot prompting: "*This challenge echoes similar findings in computer vision, where few-shot classification has shown that performance can be greatly enhanced by better feature representation and metric learning techniques, even under data-scarce conditions.*" We thank the reviewer for this helpful addition.

UIRmail

Arbi Haza <arbi@eng.uir.ac.id>

[Information] Manuscript ID: information-3588468 - Manuscript Resubmitted

1 message

Information Editorial Office <information@mdpi.com> Wed, Apr 23, 2025 at 6:27 PM
Reply-To: Eloise Yu <eloise.yu@mdpi.com>, Information Editorial Office <information@mdpi.com>
To: Arbi Haza Nasution <arbi@eng.uir.ac.id>
Cc: Winda Monika <windamonika@unilak.ac.id>, Aytug Onan <aytug.onan@ikcu.edu.tr>, Yohei Murakami <yohei@fc.ritsumei.ac.jp>

Dear Dr. Nasution,

Thank you very much for resubmitting the modified version of the following manuscript:

Manuscript ID: information-3588468
Type of manuscript: Article
Title: Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering
Authors: Arbi Haza Nasution *, Winda Monika, Aytug Onan, Yohei Murakami
Received: 31 Mar 2025
E-mails: arbi@eng.uir.ac.id, windamonika@unilak.ac.id, aytug.onan@ikcu.edu.tr, yohei@fc.ritsumei.ac.jp

https://susy.mdpi.com/user/manuscripts/review_info/6bdbfd7ea9322323b64a60bb6db39b77

A member of the editorial office will be in touch with you soon regarding progress of the manuscript.

Kind regards,
Information Editorial Office
Postfach, CH-4020 Basel, Switzerland
Office: Grosspeteranlage 5, CH-4052 Basel
Tel. +41 61 683 77 34 (office)
E-mail: information@mdpi.com
https://www.mdpi.com/journal/information/

*** This is an automatically generated email ***

Arbi Haza Nasution
Universitas Islam Riau
Jl. Kaharuddin Nst No.113, Simpang Tiga, Kec.
Bukit Raya, Kota Pekanbaru, Riau 28284
Pekanbaru 28284
Indonesia

INVOICE

MDPI AG
Grosspeteranlage 5
4052 Basel
Switzerland

Tel.: +41 61 683 77 34
E-Mail: billing@mdpi.com
Website: www.mdpi.com
VAT nr. CHE-115.694.943

Date of Invoice:	29 April 2025
Manuscript ID:	information-3588468
Invoice Number:	3588468
Your Order:	by e-mail (arbi@eng.uir.ac.id) on 31 March 2025
Article Title:	"Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering"
Name of co-authors:	Arbi Haza Nasution, Winda Monika, Aytug Onan and Yohei Murakami Additional Author Information
Institutional Open Access Program (IOAP):	Ritsumeikan University
Terms of payment:	5 days
Due Date:	4 May 2025
License:	CC BY

Description	Currency	Amount
Article Processing Charges	CHF	1 600.00
IOAP discount (10%)	CHF	(160.00)
Author Voucher discount code (90c7ece2344ff849)	CHF	(100.00)
Author Voucher discount code (5595277cbb0ecc11)	CHF	(50.00)
Author Voucher discount code (cb5f8acea93f34a7)	CHF	(100.00)
Author Voucher discount code (7a0835f2cff5efa1)	CHF	(100.00)
Author Voucher discount code (aed873ab673d355d)	CHF	(50.00)
Author Voucher discount code (e3f5ec2244bab870)	CHF	(100.00)
Author Voucher discount code (da3fa302a7fe30ca)	CHF	(50.00)
Author Voucher discount code (6f4ec29c3dcca9a3)	CHF	(50.00)
Author Voucher discount code (e187869bdf8d0760)	CHF	(100.00)
Subtotal without VAT	CHF	740.00
VAT (0%)	CHF	0.00
Total with VAT	**CHF**	**740.00**

Accepted Payment Methods

1. Online Payment by Credit Card in Swiss Francs (CHF)

Please visit https://payment.mdpi.com/3521367 to pay by credit card. We accept payments in Swiss Francs (CHF) made through VISA, MasterCard, Maestro, American Express, Diners Club, Discover, China UnionPay and Alipay+.

2. Paypal in Swiss Francs (CHF)

Please visit https://payment.mdpi.com/payment/paypal and enter the payment details. Note that the fee for using Paypal is 5% of the invoiced amount.

3. Wire Transfer in Swiss Francs (CHF)

Important: **Please provide the Manuscript ID (information-3588468) when transferring the payment**

Payment in CHF must be made by wire transfer to the MDPI bank account. Banks fees must be paid by the customer for both payer and payee so that MDPI can receive the full invoiced amount.

IBAN: CH74 0023 3233 2227 2101 Y
SWIFT Code / BIC (Wire Transfer Address): UBSWCHZH80A

Beneficiary's Name: MDPI AG
Beneficiary's Address: Grosspeteranlage 5, 4052 Basel, Switzerland
Bank Account Number (CHF Account for MDPI): 0233 00222721.01Y
Bank Name: UBS Switzerland AG
Bank Address:

UBS Switzerland AG
Bahnhofstrasse 45
8001 Zürich
Switzerland

For detailed payment instruction, or for more alternative payment methods, visit the website at https://www.mdpi.com/about/payment.

Thank you for choosing MDPI.

UIRmail

Arbi Haza <arbi@eng.uir.ac.id>

[Information] Manuscript ID: information-3588468; doi: 10.3390/info16050366. Paper has been published.

4 messages

information@mdpi.com <information@mdpi.com> Tue, Apr 29, 2025 at 9:59 PM
Reply-To: eloise.yu@mdpi.com, information@mdpi.com
To: arbi@eng.uir.ac.id, windamonika@unilak.ac.id, aytug.onan@ikcu.edu.tr, yohei@fc.ritsumei.ac.jp
Cc: billing@mdpi.com, website@mdpi.com, information@mdpi.com, sierra.liu@mdpi.com, eloise.yu@mdpi.com, amanda.liu@mdpi.com

Dear Authors,

We are pleased to inform you that your article "Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering" has been published in Information and is available online at the following links:

Website: https://www.mdpi.com/2078-2489/16/5/366
PDF Version: https://www.mdpi.com/2078-2489/16/5/366/pdf
The meta data of your article, the manuscript files and a publication certificate are available at the following websites (only available to corresponding authors after login):
https://susy.mdpi.com/user/manuscripts/review_info/6bdbfd7ea9322323b64a60bb6db39b77

Please note that this is an early access version. The complete PDF, HTML, and XML versions will be available soon. Please take a moment to check that everything is correct. You can reply to this email if there is a problem. If there are any errors, please note that all authors must follow MDPI's policy on updating published papers, which can be found here: https://www.mdpi.com/ethics#16.

To encourage open scientific discussions and increase the visibility of published articles, MDPI recently implemented interactive commenting and recommendation functionalities on all article webpages (side bar on the right). We encourage you to forward the article link to your colleagues and peers.

We also encourage you to set up your profile at www.SciProfiles.com, MDPI's researcher network platform. Articles you publish with MDPI will be linked to your SciProfiles page, where colleagues and peers will be able to see all of your publications and citations, as well as your other academic contributions. Please also feel free to send us feedback on the platform to allow us to improve it and ensure that it is useful for scientific communities.

You can also share the paper on various social networks by clicking the links on the article webpage. Alternatively, our Editorial Office can post an announcement of your article on our X channel (for this, please send us a description of up to 200 characters including spaces). Please note that our service Scitations.net will automatically notify authors cited in your article. For further paper promotion guidelines, please refer to the following link: https://www.mdpi.com/authors/promoting.

We would like to take this opportunity to invite you to contribute to the dissemination of high-quality research by joining us as a Volunteer Reviewer at https://susy.mdpi.com/volunteer_reviewer/step/1. As a Volunteer Reviewer, you can contribute to the peer review process and directly apply to review papers that interest you. MDPI partners with Web of Science Reviewer Recognition Services (formerly Publons) (https://clarivate.com/products/scientific-and-academic-research/research-publishing-solutions/reviewer-recognition-service/)
to recognize reviewers. For well-prepared review reports submitted in a timely manner, we also provide article processing charge discount vouchers.

If you would like to remain updated about new issue releases of Information, please enter your e-mail address in the box at https://www.mdpi.com/journal/information/toc-alert/ to receive notifications. After issue release, a version of your paper including the issue cover will be available to download from the article abstract page.

To order high-quality reprints of your article in quantities of 25–1000, visit the following link: https://www.mdpi.com/2078-2489/16/5/366/reprints

We support the multidisciplinary preprint platform Preprints, which permanently archives full text documents and datasets of working papers in all subject areas. Posting on the platform is entirely free of charge, and full details can be viewed at http://www.preprints.org.

To help us improve our Production and English Editing services, provided as part of MDPI's editorial process, please take a few minutes to complete the following survey: https://www.surveymonkey.com/r/CMDKPKJ (for Production and English Editing services).

Thank you for choosing Information to publish your work, and we look forward to receiving further contributions from your research group in the future.

Kind regards,

--
MDPI
Postfach, CH - 4020 Basel, Switzerland
Office: Grosspeteranlage 5, 4052 Basel, Switzerland
Tel. +41 61 683 77 34
Fax: +41 61 302 89 18
E-mail: website@mdpi.com
https://www.mdpi.com/

Arbi Haza <arbi@eng.uir.ac.id> Tue, Apr 29, 2025 at 10:12 PM
To: eloise.yu@mdpi.com, information@mdpi.com
Cc: windamonika@unilak.ac.id, aytug.onan@ikcu.edu.tr, yohei@fc.ritsumei.ac.jp, billing@mdpi.com, website@mdpi.com, information@mdpi.com, sierra.liu@mdpi.com, eloise.yu@mdpi.com, amanda.liu@mdpi.com

Dear Editor,

If possible, I would like to replace Figure 2 with the attached image to reflect reviewer 1's comment in the second round review report.

Best Regards,

Assoc. Prof. Dr. Arbi Haza Nasution, B.IT (Hons), M.IT
Director of Directorate of Research and Community Service
Universitas Islam Riau
Jl. Kaharuddin Nasution 113 Pekanbaru Riau
https://arbihaza.com

[Quoted text hidden]

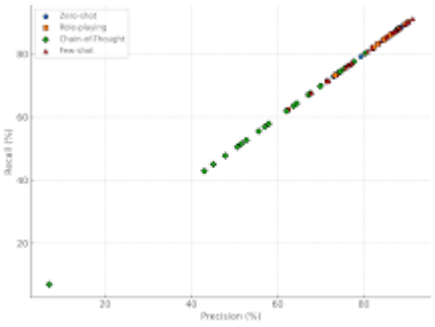

Figure 2.png
119K

Amanda Liu <amanda.liu@mdpi.com> Wed, Apr 30, 2025 at 7:44 AM
To: Arbi Haza <arbi@eng.uir.ac.id>
Cc: eloise.yu@mdpi.com, information@mdpi.com, windamonika@unilak.ac.id, aytug.onan@ikcu.edu.tr, yohei@fc.ritsumei.ac.jp, billing@mdpi.com, website@mdpi.com, sierra.liu@mdpi.com

Dear Authors,

Thank you for your kind email. This is Amanda Liu, the Managing Editor of Information Journal.

If it's just a change in color, we do not encourage an update at this stage. Thank you for your understanding and cooperation. Congratulations again on the publication of your article.

Best regards,
Ms. Amanda Liu
Managing Editor
E-Mail: amanda.liu@mdpi.com

MDPI Branch Office, Wuhan
No. 688, Jinghan Avenue, Floor 54, Wuhan Hang Lung Plaza Office Tower,
Hubei Province, 430030 Wuhan, China
Tel.: 027 8780 8658

Good News:
Information received an increased CiteScore of 6.9
Information received an Impact Factor for 2023 of 2.4
--
"/Information/ *Top Cited Papers in the past 2 years*" :
"A Comparison of Undersampling, Oversampling, and SMOTE Methods for Dealing with Imbalanced Classification in Educational Data Mining":
https://www.mdpi.com/2078-2489/14/1/54
"Smart Contracts in Blockchain Technology: A Critical Review":
https://www.mdpi.com/2078-2489/14/2/117
--
MDPI
Information Editorial Office
Information@mdpi.com
http://www.mdpi.com/journal/information/
Data Protection Notes: https://www.mdpi.com/about/data-protection
MDPI's headquarters are located in Basel, Switzerland. More information is available here: https://www.mdpi.com/about/contact

On 2025/4/29 23:12, Arbi Haza wrote:

> CAUTION - EXTERNAL: This email originated from outside of MDPI organisation. BE CAUTIOUS especially to click links or open attachments.
>
> Dear Editor,
>
> If possible, I would like to replace Figure 2 with the attached image

to reflect reviewer 1's comment in the second round review report.

Best Regards,

Assoc. Prof. Dr. Arbi Haza Nasution, B.IT <http://b.it/> (Hons), M.IT <http://m.it/> Director of Directorate of Research and Community Service Universitas Islam Riau Jl. Kaharuddin Nasution 113 Pekanbaru Riau https://arbihaza.com <http://arbihaza.com/>

On Tue, Apr 29, 2025 at 9:59 PM <information@mdpi.com <mailto:information@mdpi.com>> wrote:

Dear Authors,

We are pleased to inform you that your article "Benchmarking 21 Open-Source Large Language Models for Phishing Link Detection with Prompt Engineering" has been published in Information and is available online at the following links:

Website: https://www.mdpi.com/2078-2489/16/5/366 PDF Version: https://www.mdpi.com/2078-2489/16/5/366/pdf
The meta data of your article, the manuscript files and a publication certificate are available at the following websites (only available to corresponding authors after login): https://susy.mdpi.com/user/manuscripts/review_info/6bdbfd7ea9322323b64a60bb6db39b77

Please note that this is an early access version. The complete PDF, HTML, and XML versions will be available soon. Please take a moment to check that everything is correct. You can reply to this email if there is a problem. If there are any errors, please note that all authors must follow MDPI's policy on updating published papers, which can be found here: https://www.mdpi.com/ethics#16.

To encourage open scientific discussions and increase the visibility of published articles, MDPI recently implemented interactive commenting and recommendation functionalities on all article webpages (side bar on the right). We encourage you to forward the article link to your colleagues and peers.

We also encourage you to set up your profile at www.SciProfiles.com <http://www.SciProfiles.com>, MDPI's researcher network platform. Articles you publish with MDPI will be linked to your SciProfiles page, where colleagues and peers will be able to see all of your publications and citations, as well as your other academic contributions. Please also feel free to send us feedback on the platform to allow us to improve it and ensure that it is useful for scientific communities.

You can also share the paper on various social networks by clicking the links on the article webpage. Alternatively, our Editorial Office can post an announcement of your article on our X channel (for this, please send us a description of up to 200 characters including spaces). Please note that our service Scitations.net will automatically notify authors cited in your article. For further paper promotion guidelines, please refer to the following link: https://www.mdpi.com/authors/promoting.

We would like to take this opportunity to invite you to contribute to the dissemination of high-quality research by joining us as a Volunteer Reviewer at https://susy.mdpi.com/volunteer_reviewer/step/1. As a Volunteer Reviewer, you can contribute to the peer review process and directly apply to review papers that interest you. MDPI partners with Web of Science Reviewer Recognition Services (formerly Publons) (https://clarivate.com/products/scientific-and-academic-research/research-publishing-solutions/reviewer-recognition-service/) to recognize reviewers. For well-prepared review reports submitted in a timely manner, we also provide article processing charge discount vouchers.

If you would like to remain updated about new issue releases of Information, please enter your e-mail address in the box at https://www.mdpi.com/journal/information/toc-alert/ to receive notifications. After issue release, a version of your paper including the issue cover will be available to download from the article abstract page.

To order high-quality reprints of your article in quantities of 25–1000, visit the following link: https://www.mdpi.com/2078-2489/16/5/366/reprints

We support the multidisciplinary preprint platform Preprints, which permanently archives full text documents and datasets of working papers in all subject areas. Posting on the platform is entirely free of charge, and full details can be viewed at http://www.preprints.org.

To help us improve our Production and English Editing services, provided as part of MDPI's editorial process, please take a few minutes to complete the following survey: https://www.surveymonkey.com/r/CMDKPKJ (for Production and English Editing services).

Thank you for choosing Information to publish your work, and we look forward to receiving further contributions from your research group in the future.

Kind regards,

-- MDPI Postfach, CH - 4020 Basel, Switzerland Office: Grosspeteranlage 5, 4052 Basel, Switzerland Tel. +41 61 683 77 34 Fax: +41 61 302 89 18 E-mail: website@mdpi.com <mailto:website@mdpi.com> https://www.mdpi.com/

Arbi Haza <arbi@eng.uir.ac.id> Wed, Apr 30, 2025 at 8:18 AM
To: Amanda Liu <amanda.liu@mdpi.com>
Cc: eloise.yu@mdpi.com, Information Editorial Office <information@mdpi.com>, windamonika <windamonika@unilak.ac.id>, Aytug Onan <aytug.onan@ikcu.edu.tr>, MURAKAMI YOHEI <yohei@fc.ritsumei.ac.jp>, billing <billing@mdpi.com>, website@mdpi.com, sierra.liu@mdpi.com

I see. Thank you for the clarification.

Best Regards,

Assoc. Prof. Dr. Arbi Haza Nasution, B.IT (Hons), M.IT
Director of Directorate of Research and Community Service
Universitas Islam Riau
Jl. Kaharuddin Nasution 113 Pekanbaru Riau
https://arbihaza.com
[Quoted text hidden]