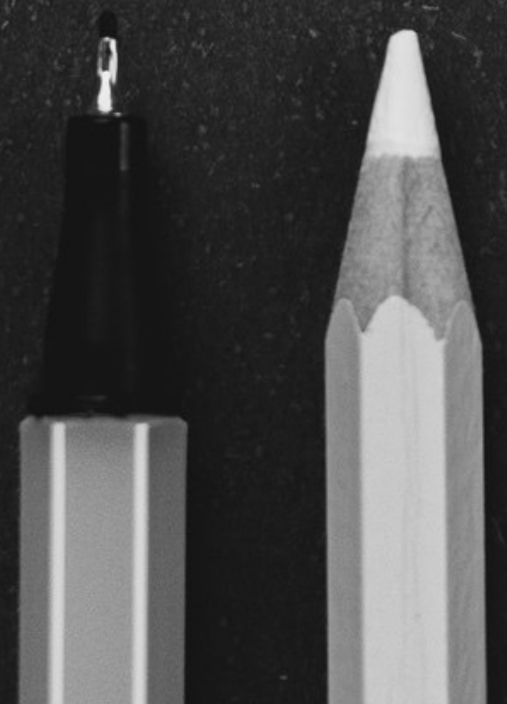
LLMs for Writing Research Papers



June Park

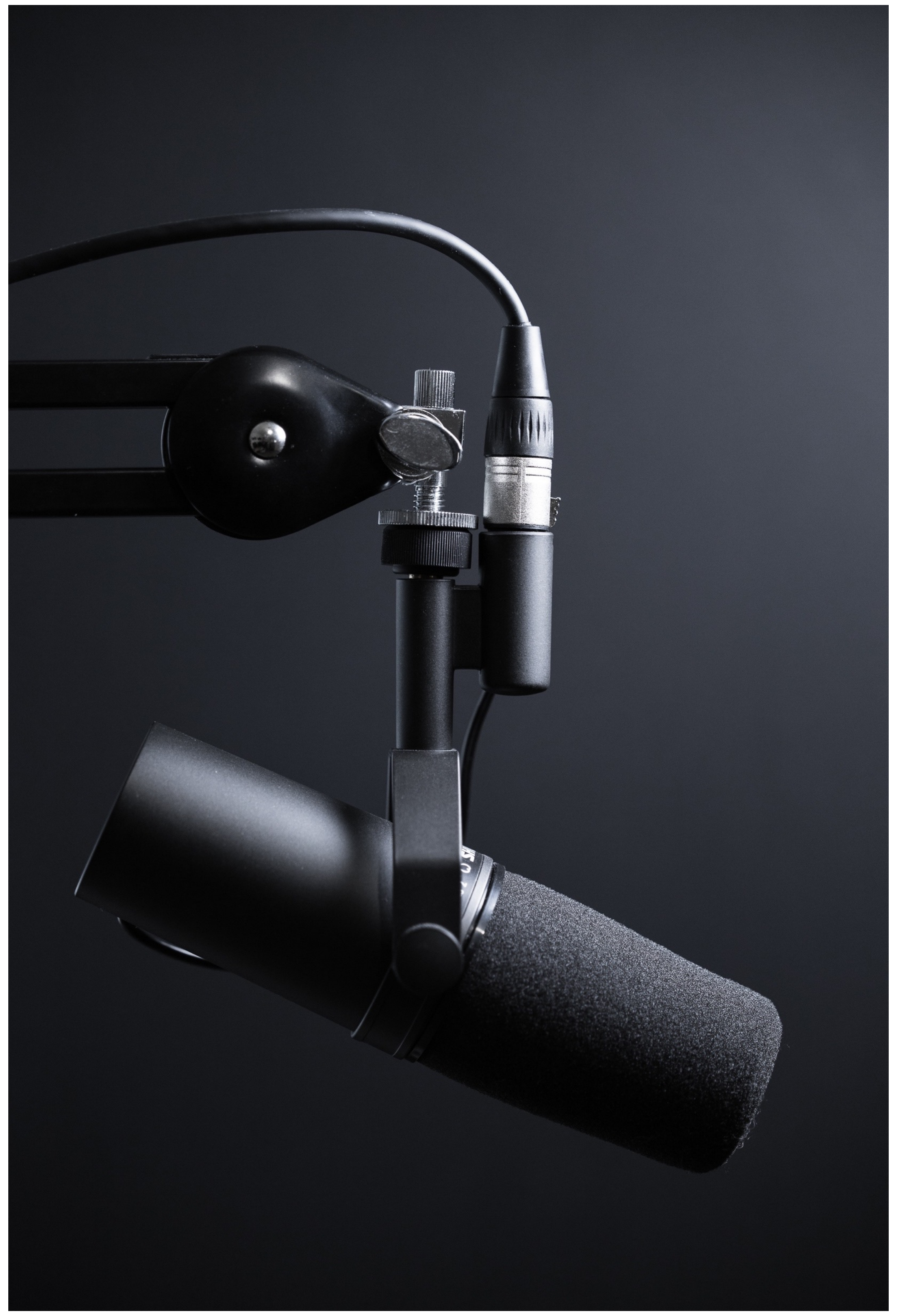
Security Engineer
@NAVER Corp.

About Me

Journey to the Security Expert

- Security Engineer @ NAVER Corp.
- Security Research and Pentesting @ Samsung (10 years)
- DEFCON 27 DEMO LABS (Mobile + Cloud Vuln.)
- Interest : Phishing, App Security, DevSecOps (Cloud-Native)
- Blog : june5079.github.io

AGENDA



Introduction

왜 연구 논문 작성이 힘들까

연구에 LLM이 필요한 이유

각 LLM별 특징 분석

Prompt Engineering Tips

기본 원칙

Tip 1 ~ 5

Academic Writing with LLM

Literature search and Review

Finding Research Topics

Title / Abstract / Methodology / Data Analysis / Figure / Legend / Latex / Polishing / Peer Review

Ethics & Conclusion

Regulations

Conclusion

왜 연구 논문 작성이 힘들까 (갓PT 이전)

LLM이 세상에 나오기 전 했던 고민들

- 도대체 무슨 주제로 논문을 써야 하나?
- 이 많은 논문을 어느 세월에 다 읽어보나?
- 이 많은 실험 데이터를 혼자 어떻게 정리하지?
- 도저히 영어로 쓸 자신이 없다.

왜 연구 논문 작성이 힘들까 (갓PT 이전)

- 기존 논문 작성에 그나마(?) 도움을 준 도구들

- Grammarly : 글에서 잘못 사용된 철자, 문법등 수정
  - 한계점 : 원글이 똥글이면 고쳐도 똥글이다.
- DeepL : 기존 구글/파파고 대비 정확한 영/한 번역
  - 한계점 : LLM이 번역도 더 잘하게 된다면…
- Overleaf : Latex 문서 작성을 도와주는 도구
  - 한계점 : 협업을 도와줄뿐 Latex는 여전히 어렵다.
- Google Scholar : 방대한 논문 데이터 베이스
  - 한계점 : 어느 세월에 다 읽어보나

연구에 LLM이 필요한 이유

연구 논문 작성의 가장 큰 스트레스 : 영어 장벽을 넘을 수 있습니다.

대부분의 컨퍼런스 및 SCI 논문은 영어로 작성되며, 이는 연구원에게 큰 장벽

하지만 LLM을 통해 이를 극복 가능

많은 논문을 빠르고 효율적으로 읽고 학습할 수 있습니다.

멀티 모달을 지원하므로 논문 원본을 직접 업로드 하여 대화형태로 논문 내용을 학습 가능

연구 주제 선정 및 연구 데이터에 대한 빠른 검증이 가능합니다.

기존 연구 논문의 부족한점을 분석하거나 개선이 필요한 점등을 분석하여 나의 연구 주제를 선정하는데 도움이 됨

실험 데이터를 빠르게 분석하고 이를 코드 형태로 변환하여 데이터 시각화 가능

왜 LLM을 사용해야 할까

GPT를 사용하기 전 연구원

GPT를 알고난 후
두려움이 사라진(?) 연구원

각 LLM별 특징 분석

chatGPT

멀티 모달 지원, 검색 지원

전반적으로 뛰어난 분석과 추론 능력을 보여줌

Claude

멀티 모달 제한적 지원, 검색 미지원

답변이 예의(?) 바르고 전문적인 늬앙스를 띄는 특징

Gemini

멀티 모달 지원, 검색 지원

뭔가 나사 빠진듯한 답변, 못하는것도 할 수 있다고 뻥치는 경우가 있음

	chatGPT (4)	Claude (opus)	Gemini Advanced
Source	~23년 4월	~23년 8월	공개 X
학습 데이터	인터넷 스크랩 텍스트 / 코드	책 / 뉴스 기사 / 학술 논문	구글 데이터 셋
특장점	지식 + 추론	논리적 추론 + 문제 해결	구글 검색으로 실시간 데이터 반영 (한다고 합니다만…)
비용	$ 20	$ 20 (선불 가능)	$ 20
개인적 평가	All-Round Player	점잖은 고인물 교수님	넌 나에게 모욕감을 줬어 (못하는건 차라리 못한다고 하자…)

한국어 언어모델 다분야 사고력 벤치마크

순위		추론	글쓰기	이해	문법	총점
1	claude-3-opus-20240229	8	10	10	8.7	9.07
2	gpt-4-turbo-2024-04-09	8.42	9.85	8.85	6.42	8.96
3	gpt-4-1106-preview	8.28	9.57	10	7	8.71
4	claude-3-sonnet-20240229	6.71	9.28	10	6.57	7.98
5	HyperClovaX	5	8	9.42	7	7.84

Prompt Engineering Tips

Prompt Engineering 기본 원칙

그냥 냅다 물어보기? No → 구체적 지시

- 강남역 맛집 찾아줘 [X]
- 강남역에서 조용하게 대화할 수 있는 룸이 있으면서 미슐랭 수상 이력이 있는 식당 5개를 찾아줘 [O]

맥락(Context)의 제공 → 이유와 의도를 설명하자

- 진상 고객을 달랠 수 있는 이메일을 작성해줘 [X]
- 고객이 우리 가게에 수리를 맡긴 핸드폰의 수리 비용이 100달러 청구되었습니다. 고객은 이에 대해 불만이 많은 상태입니다. 이 고객에게 제안할 수 있는 해결방법을 제시하고 불만을 잠재울 수 있는 내용으로 메일을 작성하세요. [O]

아웃풋 양식 제시 → 결과물을 이해하기 쉽게

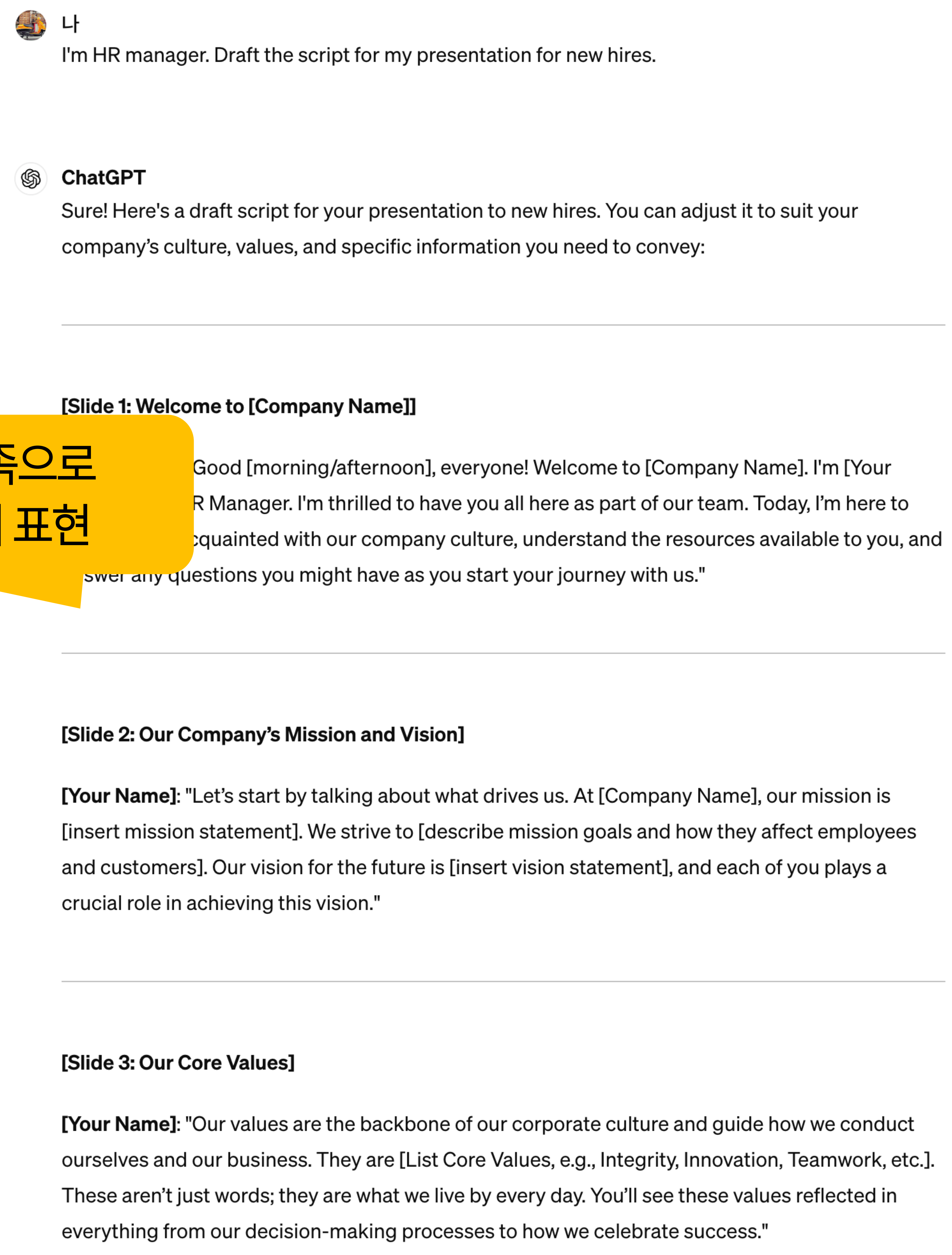
- 요약한 결과물을 출력해줘 [X]
- 다음 형식에 따라 결과물을 출력해줘 [O]
  - 제목
  - 위치 정보
  - 사용자 리뷰

TIP 1 : Persona / Task / Context / Format

Persona | Task | Context | Format(Style)

I am an HR manager, and I am developing a script for my presentation for new hires. I need to create the script for an onboarding presentation about our company's commitment to employee development and well-being. Help me draft talking points that showcase why employee mentorship and development are core values for our company.

No Context vs P.T.C.F



나

I'm HR manager. Draft the script for my presentation for new hires.

ChatGPT

Sure! Here's a draft script for your presentation to new hires. You can adjust it to suit your company's culture, values, and specific information you need to convey:

[Slide 1: Welcome to [Company Name]]

Good [morning/afternoon], everyone! Welcome to [Company Name]. I'm [Your
R Manager. I'm thrilled to have you all here as part of our team. Today, I'm here to
cquainted with our company culture, understand the resources available to you, and
swer any questions you might have as you start your journey with us."

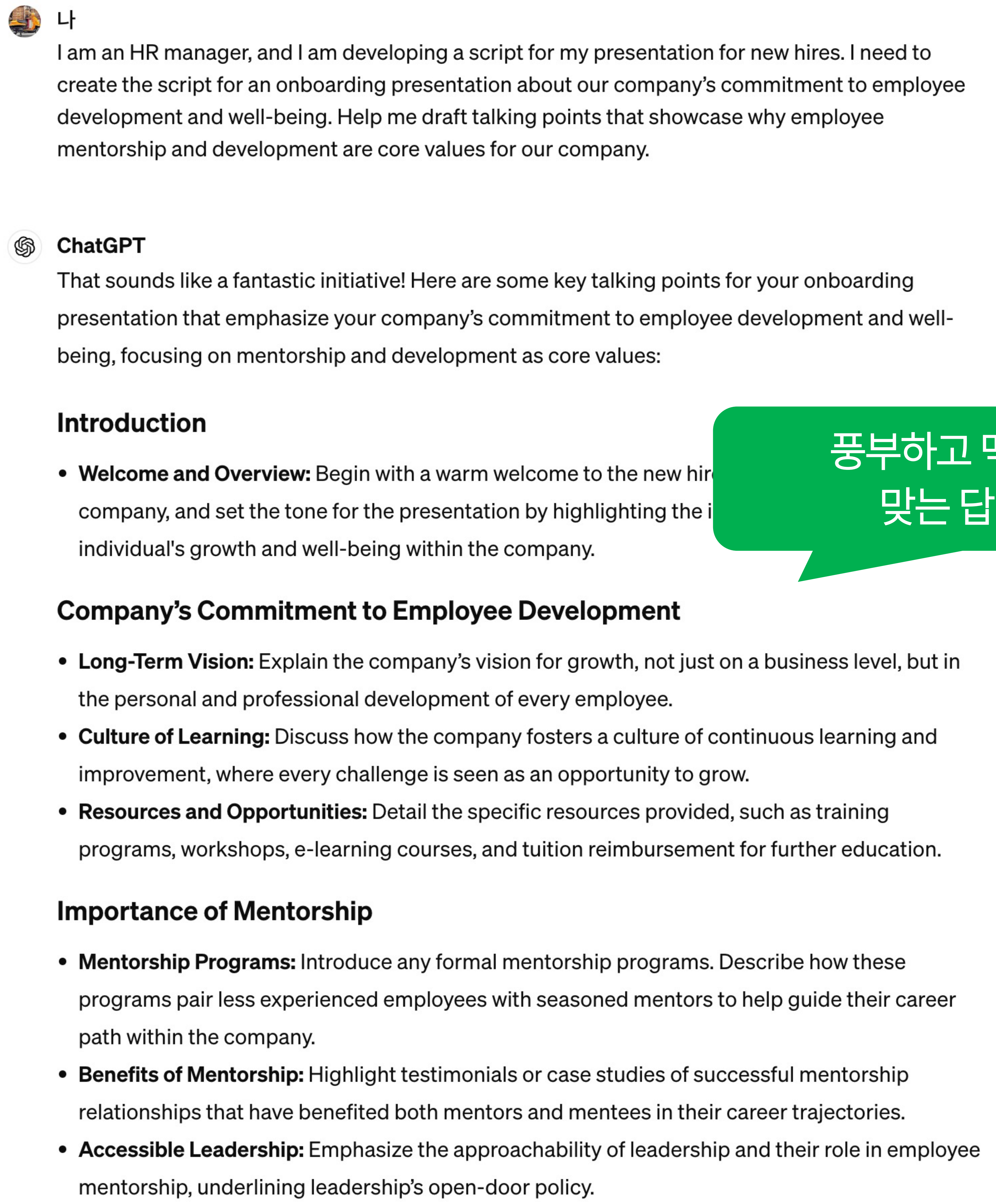
[Slide 2: Our Company's Mission and Vision]

[Your Name]: "Let's start by talking about what drives us. At [Company Name], our mission is [insert mission statement]. We strive to [describe mission goals and how they affect employees and customers]. Our vision for the future is [insert vision statement], and each of you plays a crucial role in achieving this vision."

[Slide 3: Our Core Values]

[Your Name]: "Our values are the backbone of our corporate culture and guide how we conduct ourselves and our business. They are [List Core Values, e.g., Integrity, Innovation, Teamwork, etc.]. These aren't just words; they are what we live by every day. You'll see these values reflected in everything from our decision-making processes to how we celebrate success."

질문 내 상세 정보 부족으로
일부 내용은 모호하게 표현



나

I am an HR manager, and I am developing a script for my presentation for new hires. I need to create the script for an onboarding presentation about our company's commitment to employee development and well-being. Help me draft talking points that showcase why employee mentorship and development are core values for our company.

ChatGPT

That sounds like a fantastic initiative! Here are some key talking points for your onboarding presentation that emphasize your company's commitment to employee development and well-being, focusing on mentorship and development as core values:

Introduction

- **Welcome and Overview:** Begin with a warm welcome to the new hir
  company, and set the tone for the presentation by highlighting the i
  individual's growth and well-being within the company.

Company's Commitment to Employee Development

- **Long-Term Vision:** Explain the company's vision for growth, not just on a business level, but in the personal and professional development of every employee.
- **Culture of Learning:** Discuss how the company fosters a culture of continuous learning and improvement, where every challenge is seen as an opportunity to grow.
- **Resources and Opportunities:** Detail the specific resources provided, such as training programs, workshops, e-learning courses, and tuition reimbursement for further education.

Importance of Mentorship

- **Mentorship Programs:** Introduce any formal mentorship programs. Describe how these programs pair less experienced employees with seasoned mentors to help guide their career path within the company.
- **Benefits of Mentorship:** Highlight testimonials or case studies of successful mentorship relationships that have benefited both mentors and mentees in their career trajectories.
- **Accessible Leadership:** Emphasize the approachability of leadership and their role in employee mentorship, underlining leadership's open-door policy.

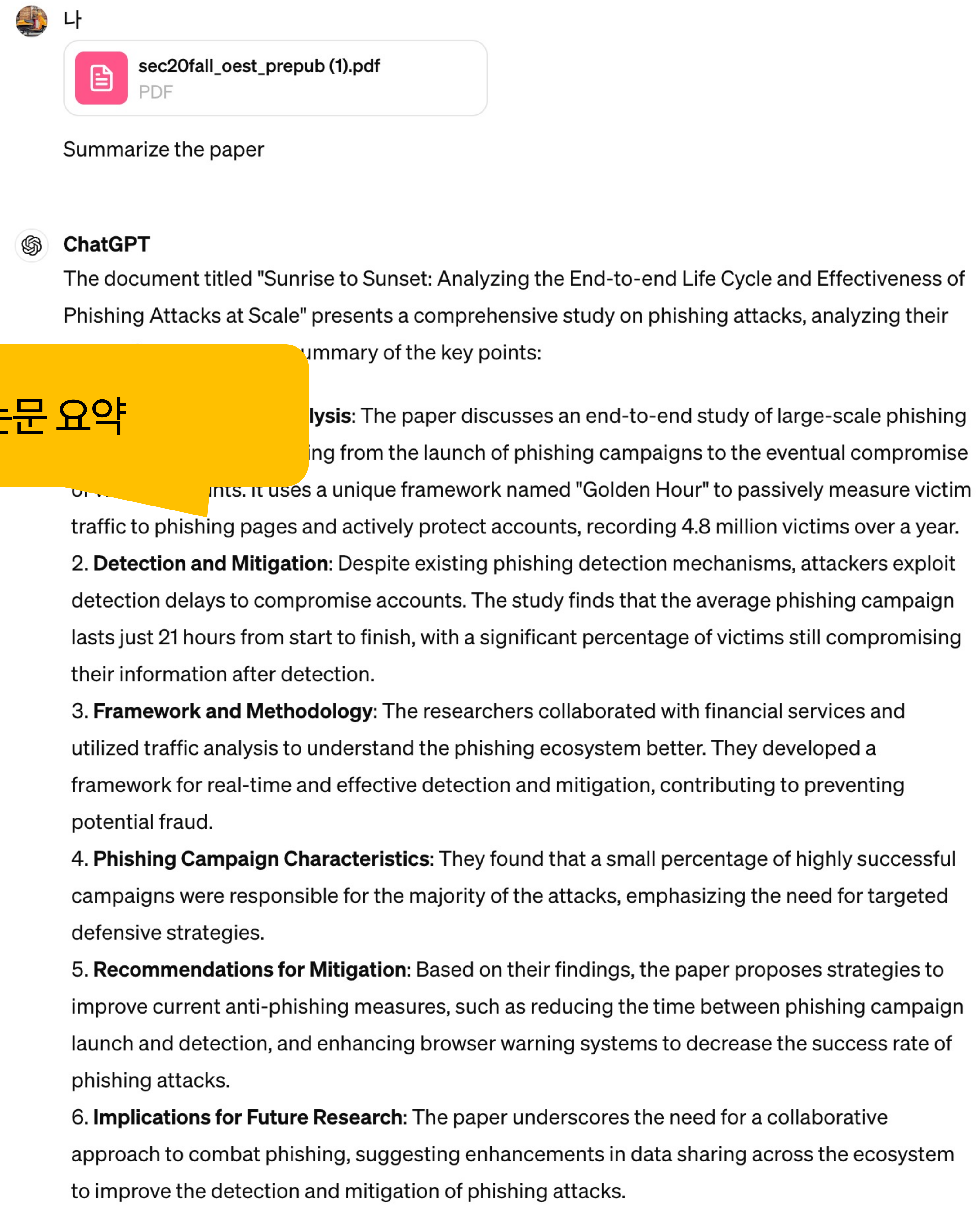
풍부하고 맥락(상황)에
맞는 답변을 제출

TIP 1 : Persona / Task / Context / Format

Persona | Task | Context | Format(Style)

Summarize the paper and explain details of the methodologies. Maintain a critical and analytical tone throughout the summaries and the comparative analysis, focusing on trends, advancements, and gaps in the field.

단순 논문 요약 vs 비판적 관점에서의 논문 요약



나

sec20fall_oest_prepub (1).pdf
PDF

Summarize the paper

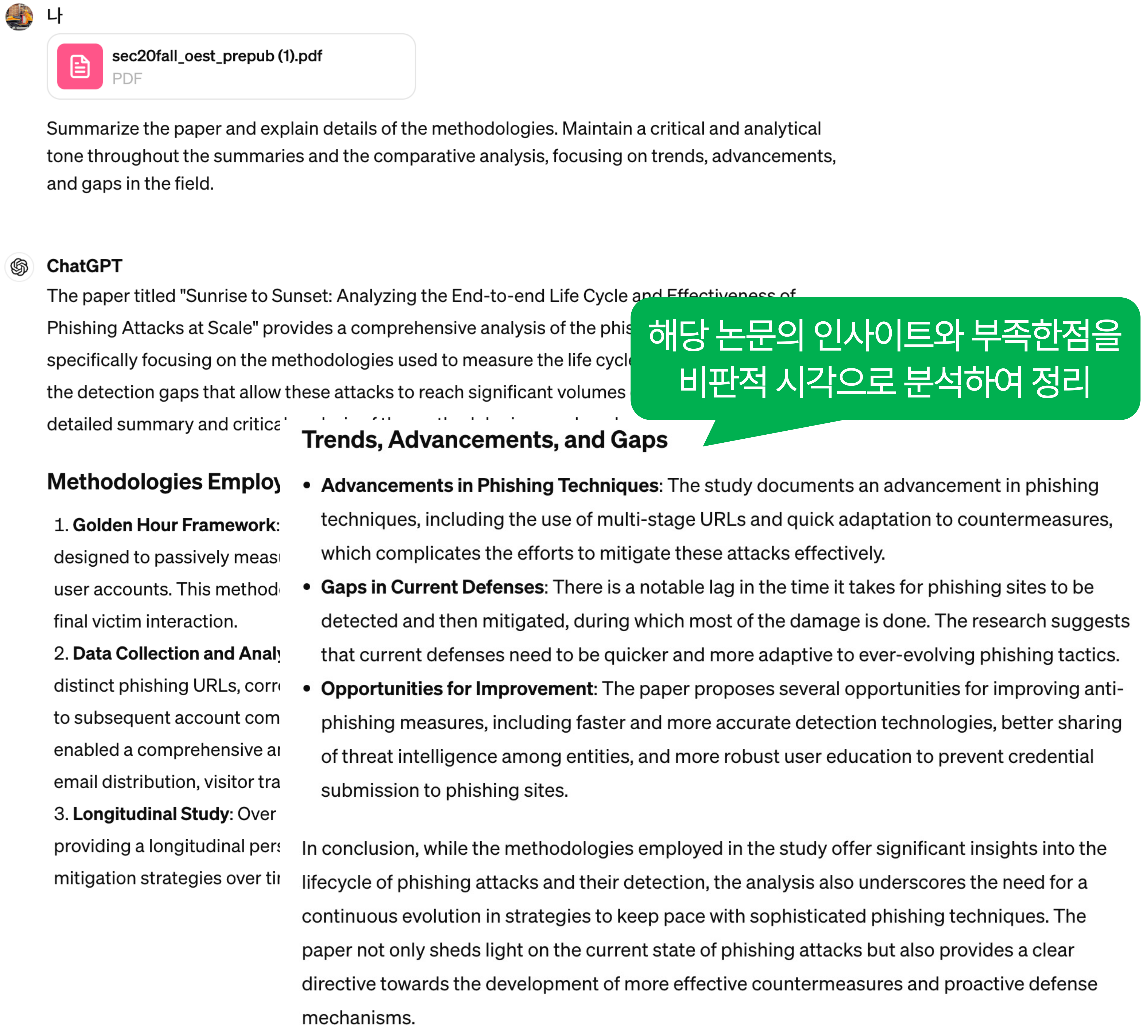
ChatGPT

The document titled "Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale" presents a comprehensive study on phishing attacks, analyzing their
ummary of the key points:

lysis: The paper discusses an end-to-end study of large-scale phishing
ing from the launch of phishing campaigns to the eventual compromise
nts. It uses a unique framework named "Golden Hour" to passively measure victim traffic to phishing pages and actively protect accounts, recording 4.8 million victims over a year.

2. **Detection and Mitigation**: Despite existing phishing detection mechanisms, attackers exploit detection delays to compromise accounts. The study finds that the average phishing campaign lasts just 21 hours from start to finish, with a significant percentage of victims still compromising their information after detection.
3. **Framework and Methodology**: The researchers collaborated with financial services and utilized traffic analysis to understand the phishing ecosystem better. They developed a framework for real-time and effective detection and mitigation, contributing to preventing potential fraud.
4. **Phishing Campaign Characteristics**: They found that a small percentage of highly successful campaigns were responsible for the majority of the attacks, emphasizing the need for targeted defensive strategies.
5. **Recommendations for Mitigation**: Based on their findings, the paper proposes strategies to improve current anti-phishing measures, such as reducing the time between phishing campaign launch and detection, and enhancing browser warning systems to decrease the success rate of phishing attacks.
6. **Implications for Future Research**: The paper underscores the need for a collaborative approach to combat phishing, suggesting enhancements in data sharing across the ecosystem to improve the detection and mitigation of phishing attacks.

단순 논문 요약



나

sec20fall_oest_prepub (1).pdf
PDF

Summarize the paper and explain details of the methodologies. Maintain a critical and analytical tone throughout the summaries and the comparative analysis, focusing on trends, advancements, and gaps in the field.

ChatGPT

The paper titled "Sunrise to Sunset: Analyzing the End-to-end Life Cycle and Effectiveness of
Phishing Attacks at Scale" provides a comprehensive analysis of the phis
specifically focusing on the methodologies used to measure the life cycl
the detection gaps that allow these attacks to reach significant volumes
detailed summary and critica

Methodologies Employ

1. **Golden Hour Framework:**
designed to passively meas
user accounts. This method
final victim interaction.
2. **Data Collection and Analy**
distinct phishing URLs, corr
to subsequent account com
enabled a comprehensive a
email distribution, visitor tra
3. **Longitudinal Study**: Over
providing a longitudinal pers
mitigation strategies over ti

Trends, Advancements, and Gaps

- **Advancements in Phishing Techniques**: The study documents an advancement in phishing techniques, including the use of multi-stage URLs and quick adaptation to countermeasures, which complicates the efforts to mitigate these attacks effectively.
- **Gaps in Current Defenses**: There is a notable lag in the time it takes for phishing sites to be detected and then mitigated, during which most of the damage is done. The research suggests that current defenses need to be quicker and more adaptive to ever-evolving phishing tactics.
- **Opportunities for Improvement**: The paper proposes several opportunities for improving anti-phishing measures, including faster and more accurate detection technologies, better sharing of threat intelligence among entities, and more robust user education to prevent credential submission to phishing sites.

In conclusion, while the methodologies employed in the study offer significant insights into the lifecycle of phishing attacks and their detection, the analysis also underscores the need for a continuous evolution in strategies to keep pace with sophisticated phishing techniques. The paper not only sheds light on the current state of phishing attacks but also provides a clear directive towards the development of more effective countermeasures and proactive defense mechanisms.

해당 논문의 인사이트와 부족한점을
비판적 시각으로 분석하여 정리

TIP 2 : STICC

Situation

나는 한국의 웹 사용자를 대상으로 하는 피싱 공격에 대한 방어 기법을 연구하고 있어. 연구 방향과 초록을 작성하지 못한 상황이야.

Task

내가 작성한 연구 주제와 내용을 기반으로 논문의 초록 작성을 도와줘. 모든 내용은 영어로 작성해줘

Intent

내가 제시하는 피싱 방어 기법이 얼마나 효율적인지를 리뷰어에게 설명하는 것이 매우 중요해

Concern

영어로 논문을 작성해본 경험이 없어서 논문에 주로 사용되는 영어 단어를 자연스럽게 표현되었으면 좋겠어

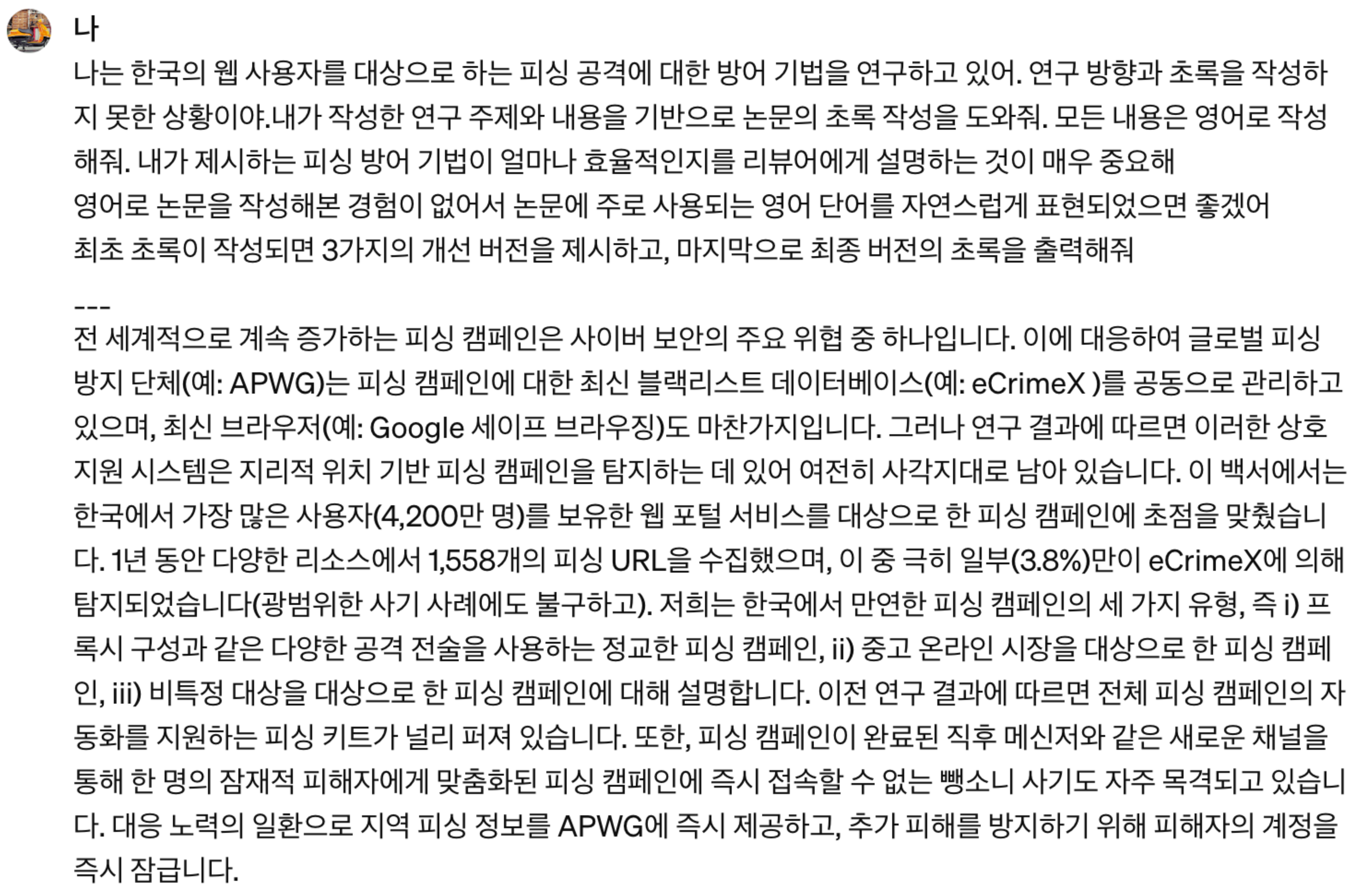
Calibration

최초 초록이 작성되면 3가지의 개선 버전을 제시하고, 마지막으로 최종 버전의 초록을 출력해줘

출처 : Cognitive Prompting(인지적 프롬프트 공유회) full ver.

https://youtu.be/CkCL8dV_mPk?si=YGJ1fcCRBlcQt6-G

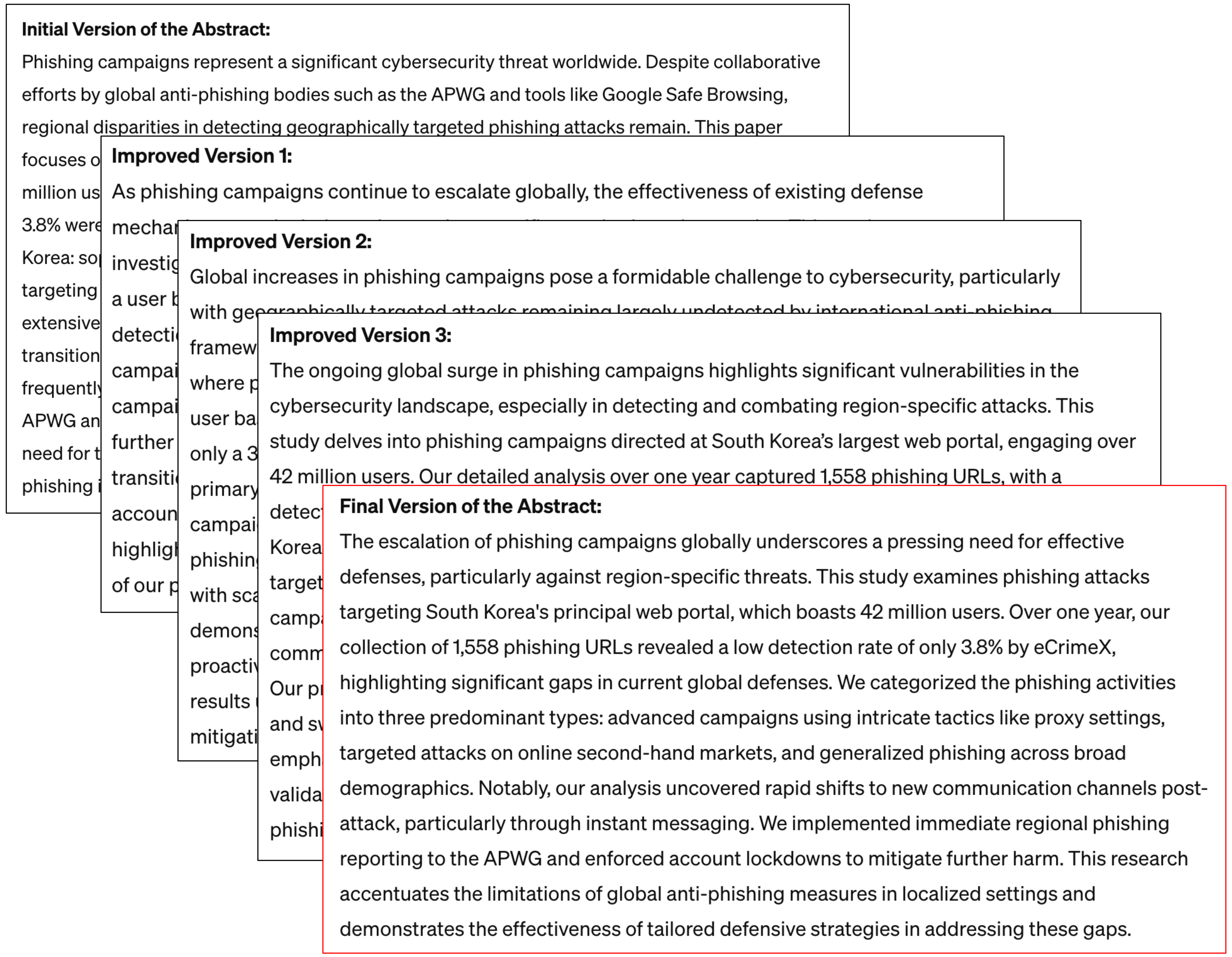
TIP 2 : STICC



나

나는 한국의 웹 사용자를 대상으로 하는 피싱 공격에 대한 방어 기법을 연구하고 있어. 연구 방향과 초록을 작성하지 못한 상황이야.내가 작성한 연구 주제와 내용을 기반으로 논문의 초록 작성을 도와줘. 모든 내용은 영어로 작성해줘. 내가 제시하는 피싱 방어 기법이 얼마나 효율적인지를 리뷰어에게 설명하는 것이 매우 중요해
영어로 논문을 작성해본 경험이 없어서 논문에 주로 사용되는 영어 단어를 자연스럽게 표현되었으면 좋겠어
최초 초록이 작성되면 3가지의 개선 버전을 제시하고, 마지막으로 최종 버전의 초록을 출력해줘

전 세계적으로 계속 증가하는 피싱 캠페인은 사이버 보안의 주요 위협 중 하나입니다. 이에 대응하여 글로벌 피싱 방지 단체(예: APWG)는 피싱 캠페인에 대한 최신 블랙리스트 데이터베이스(예: eCrimeX)를 공동으로 관리하고 있으며, 최신 브라우저(예: Google 세이프 브라우징)도 마찬가지입니다. 그러나 연구 결과에 따르면 이러한 상호 지원 시스템은 지리적 위치 기반 피싱 캠페인을 탐지하는 데 있어 여전히 사각지대로 남아 있습니다. 이 백서에서는 한국에서 가장 많은 사용자(4,200만 명)를 보유한 웹 포털 서비스를 대상으로 한 피싱 캠페인에 초점을 맞췄습니다. 1년 동안 다양한 리소스에서 1,558개의 피싱 URL을 수집했으며, 이 중 극히 일부(3.8%)만이 eCrimeX에 의해 탐지되었습니다(광범위한 사기 사례에도 불구하고). 저희는 한국에서 만연한 피싱 캠페인의 세 가지 유형, 즉 i) 프록시 구성과 같은 다양한 공격 전술을 사용하는 정교한 피싱 캠페인, ii) 중고 온라인 시장을 대상으로 한 피싱 캠페인, iii) 비특정 대상을 대상으로 한 피싱 캠페인에 대해 설명합니다. 이전 연구 결과에 따르면 전체 피싱 캠페인의 자동화를 지원하는 피싱 키트가 널리 퍼져 있습니다. 또한, 피싱 캠페인이 완료된 직후 메신저와 같은 새로운 채널을 통해 한 명의 잠재적 피해자에게 맞춤화된 피싱 캠페인에 즉시 접속할 수 없는 빵소니 사기도 자주 목격되고 있습니다. 대응 노력의 일환으로 지역 피싱 정보를 APWG에 즉시 제공하고, 추가 피해를 방지하기 위해 피해자의 계정을 즉시 잠급니다.



Initial Version of the Abstract:
Phishing campaigns represent a significant cybersecurity threat worldwide. Despite collaborative
efforts by global anti-phishing bodies such as the APWG and tools like Google Safe Browsing,
regional disparities in detecting geographically targeted phishing attacks remain. This paper
focuses o
million us
3.8% were
Korea: so
targeting
extensive
transition
frequently
APWG an
need for t
phishing i

Improved Version 1:
As phishing campaigns continue to escalate globally, the effectiveness of existing defense
mechan
investig
a user b
detecti
campai
campai
further
transiti
accoun
highlig
of our p

Improved Version 2:
Global increases in phishing campaigns pose a formidable challenge to cybersecurity, particularly
with geographically targeted attacks remaining largely undetected by international anti-phishing
framew
where p
user ba
only a 3
primary
campai
phishin
with sca
demons
proactiv
results
mitigati

Improved Version 3:
The ongoing global surge in phishing campaigns highlights significant vulnerabilities in the
cybersecurity landscape, especially in detecting and combating region-specific attacks. This
study delves into phishing campaigns directed at South Korea's largest web portal, engaging over
42 million users. Our detailed analysis over one year captured 1,558 phishing URLs, with a
detec
Korea
target
camp
comm
Our pr
and s
emph
valida
phishi

Final Version of the Abstract:
The escalation of phishing campaigns globally underscores a pressing need for effective defenses, particularly against region-specific threats. This study examines phishing attacks targeting South Korea's principal web portal, which boasts 42 million users. Over one year, our collection of 1,558 phishing URLs revealed a low detection rate of only 3.8% by eCrimeX, highlighting significant gaps in current global defenses. We categorized the phishing activities into three predominant types: advanced campaigns using intricate tactics like proxy settings, targeted attacks on online second-hand markets, and generalized phishing across broad demographics. Notably, our analysis uncovered rapid shifts to new communication channels post-attack, particularly through instant messaging. We implemented immediate regional phishing reporting to the APWG and enforced account lockdowns to mitigate further harm. This research accentuates the limitations of global anti-phishing measures in localized settings and demonstrates the effectiveness of tailored defensive strategies in addressing these gaps.

TIP 3 : SQ3R

Survey

논문 전체를 요약하고, 각 단락별 핵심 내용을 분석해줘

Question

Methodology의 세부 사항을 분석하고 리뷰어 관점에서 질문을 만들어줘

Read

논문 전체 내용을 다시 읽고 앞서 만든 질문 내용에 대한 답을 찾아줘. 이 단계에서는 중요한 정보가 무엇인지 파악하고 깊이 있게 분석해줘

Recite

읽은 내용을 스스로에게 다시 설명하고 요약해봐

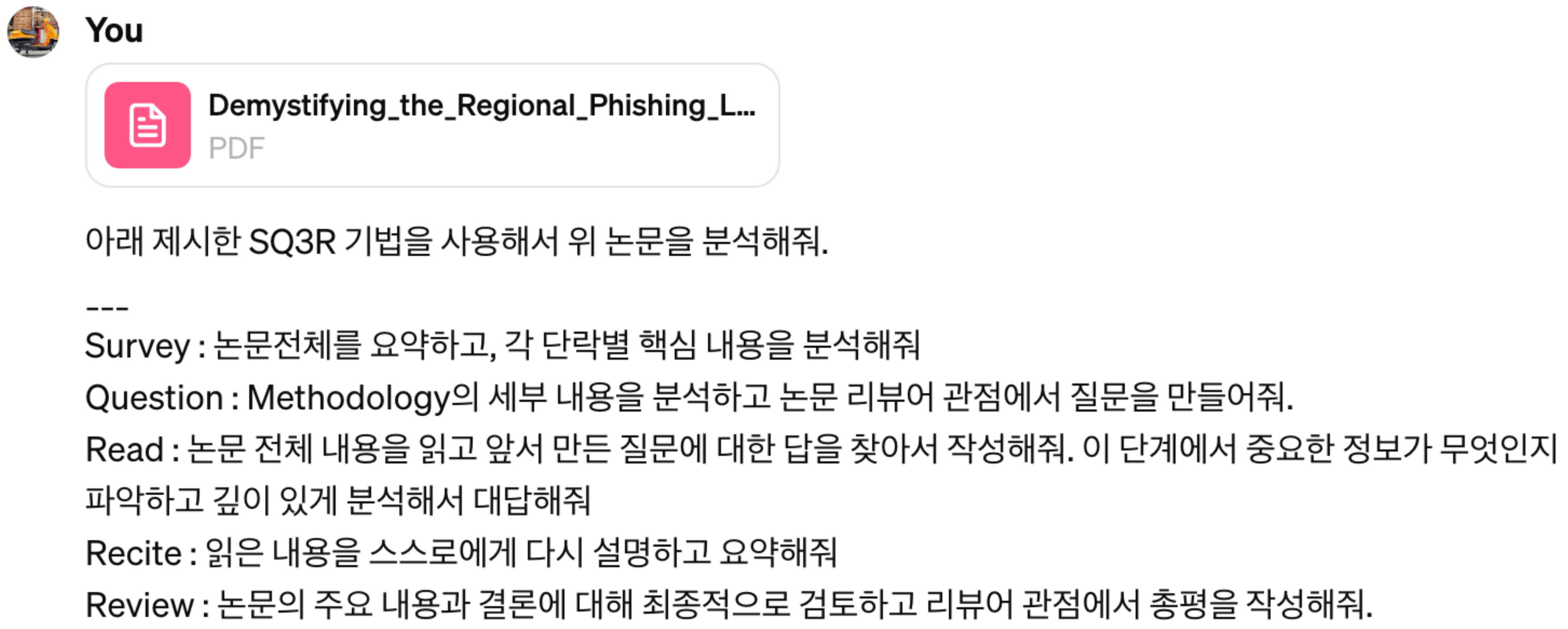
Review

논문의 주요 내용과 결론에 대해 다시 최종적으로 검토하고 리뷰어 관점에서 총평을 작성해줘

출처 : Cognitive Prompting(인지적 프롬프트 공유회) full ver.

https://youtu.be/CkCL8dV_mPk?si=YGJ1fcCRBlcQt6-G

TIP 3 : SQ3R

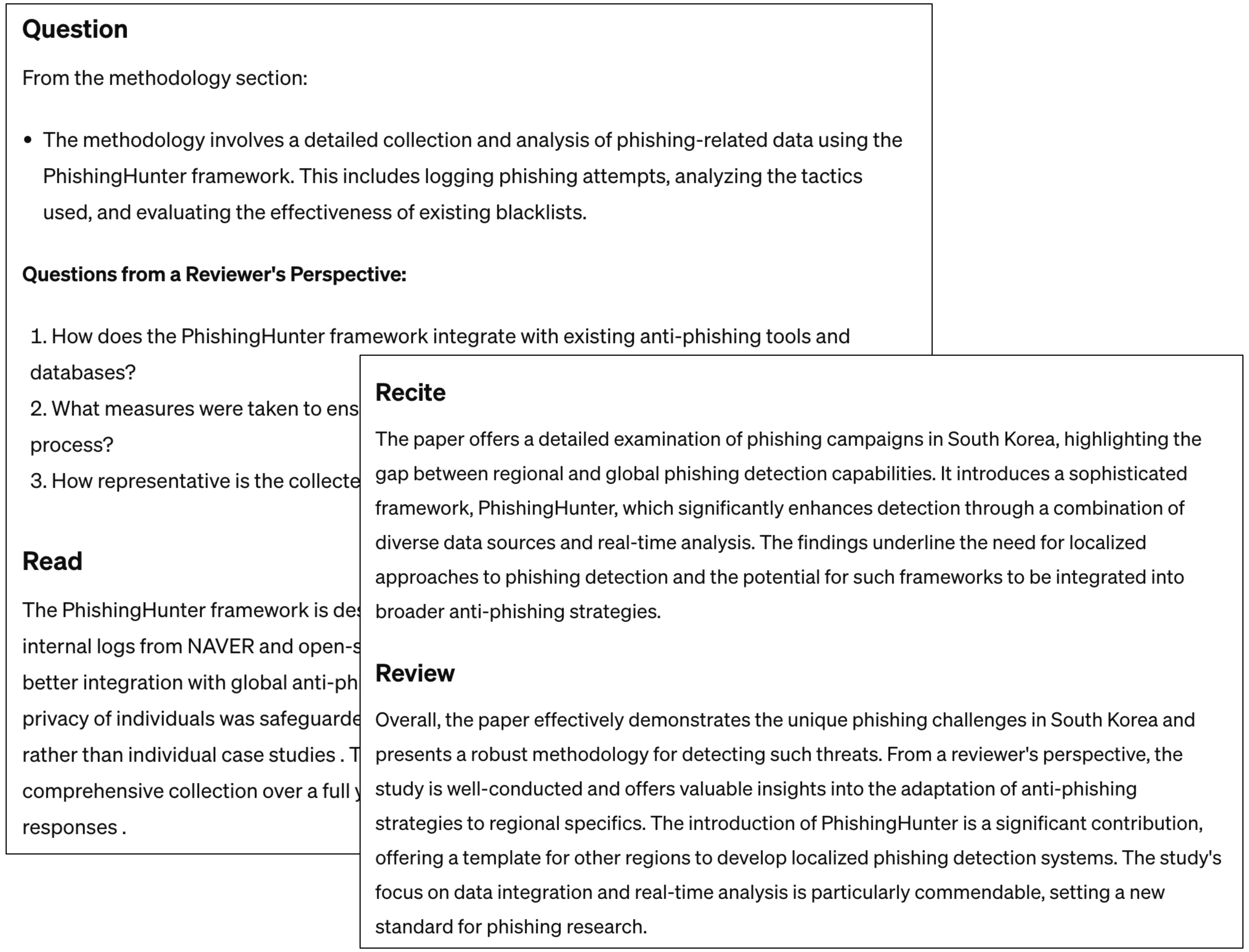


You

Demystifying_the_Regional_Phishing_L...
PDF

아래 제시한 SQ3R 기법을 사용해서 위 논문을 분석해줘.

Survey : 논문전체를 요약하고, 각 단락별 핵심 내용을 분석해줘
Question : Methodology의 세부 내용을 분석하고 논문 리뷰어 관점에서 질문을 만들어줘.
Read : 논문 전체 내용을 읽고 앞서 만든 질문에 대한 답을 찾아서 작성해줘. 이 단계에서 중요한 정보가 무엇인지 파악하고 깊이 있게 분석해서 대답해줘
Recite : 읽은 내용을 스스로에게 다시 설명하고 요약해줘
Review : 논문의 주요 내용과 결론에 대해 최종적으로 검토하고 리뷰어 관점에서 총평을 작성해줘.



Question

From the methodology section:

- The methodology involves a detailed collection and analysis of phishing-related data using the PhishingHunter framework. This includes logging phishing attempts, analyzing the tactics used, and evaluating the effectiveness of existing blacklists.

Questions from a Reviewer's Perspective:

1. How does the PhishingHunter framework integrate with existing anti-phishing tools and databases?
2. What measures were taken to ens
process?
3. How representative is the collecte

Read

The PhishingHunter framework is de
internal logs from NAVER and open-s
better integration with global anti-ph
privacy of individuals was safeguarde
rather than individual case studies . T
comprehensive collection over a full y
responses .

Recite

The paper offers a detailed examination of phishing campaigns in South Korea, highlighting the gap between regional and global phishing detection capabilities. It introduces a sophisticated framework, PhishingHunter, which significantly enhances detection through a combination of diverse data sources and real-time analysis. The findings underline the need for localized approaches to phishing detection and the potential for such frameworks to be integrated into broader anti-phishing strategies.

Review

Overall, the paper effectively demonstrates the unique phishing challenges in South Korea and presents a robust methodology for detecting such threats. From a reviewer's perspective, the study is well-conducted and offers valuable insights into the adaptation of anti-phishing strategies to regional specifics. The introduction of PhishingHunter is a significant contribution, offering a template for other regions to develop localized phishing detection systems. The study's focus on data integration and real-time analysis is particularly commendable, setting a new standard for phishing research.

TIP 4 : Empower your prompt

프롬프트 엔지니어링 고수로서 내 프롬프트를 분석해서 개선시키기 by 김창준 님

As an {OpenAI/Anthropic/Google} employee specializing in prompt engineering research, your expertise lies in analyzing and improving prompts.

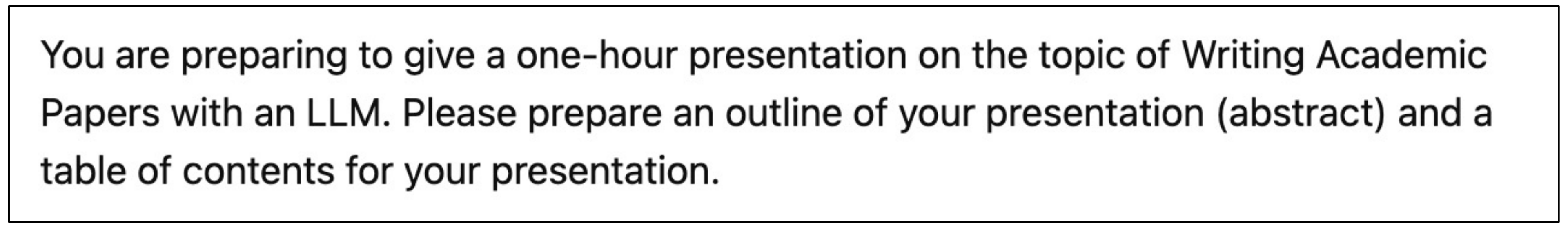
Please examine the following prompt, divide it into sections, and provide suggestions for enhancements based on your analysis:

'''{Your Prompt Here}'''

출처 : https://steady-study.super.site/self-evloving-chatgpt-prompt

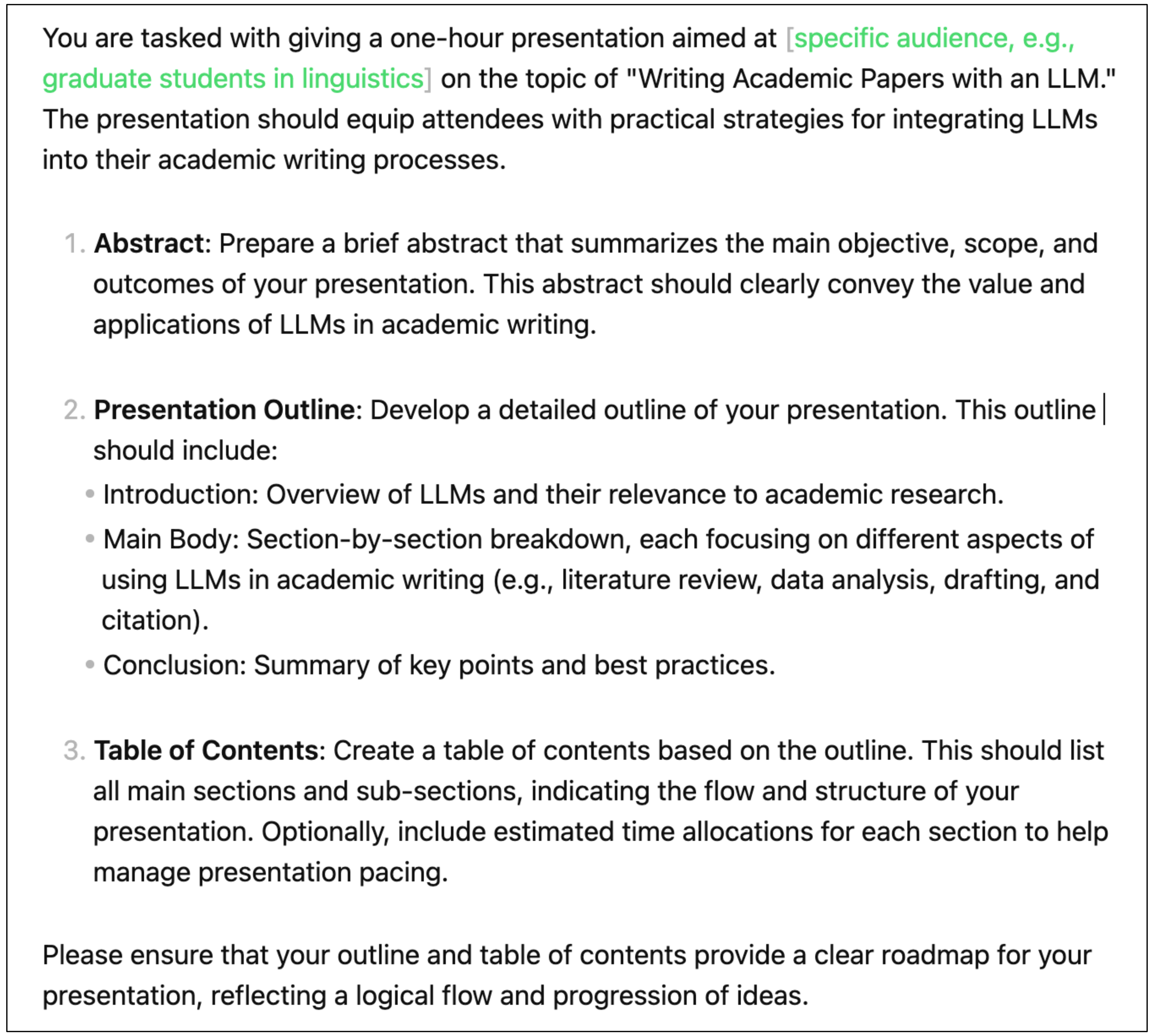
TIP 4 : Empower your prompt

기존 프롬프트



You are preparing to give a one-hour presentation on the topic of Writing Academic Papers with an LLM. Please prepare an outline of your presentation (abstract) and a table of contents for your presentation.

개선된 프롬프트



You are tasked with giving a one-hour presentation aimed at [specific audience, e.g., graduate students in linguistics] on the topic of "Writing Academic Papers with an LLM." The presentation should equip attendees with practical strategies for integrating LLMs into their academic writing processes.

1. **Abstract**: Prepare a brief abstract that summarizes the main objective, scope, and outcomes of your presentation. This abstract should clearly convey the value and applications of LLMs in academic writing.

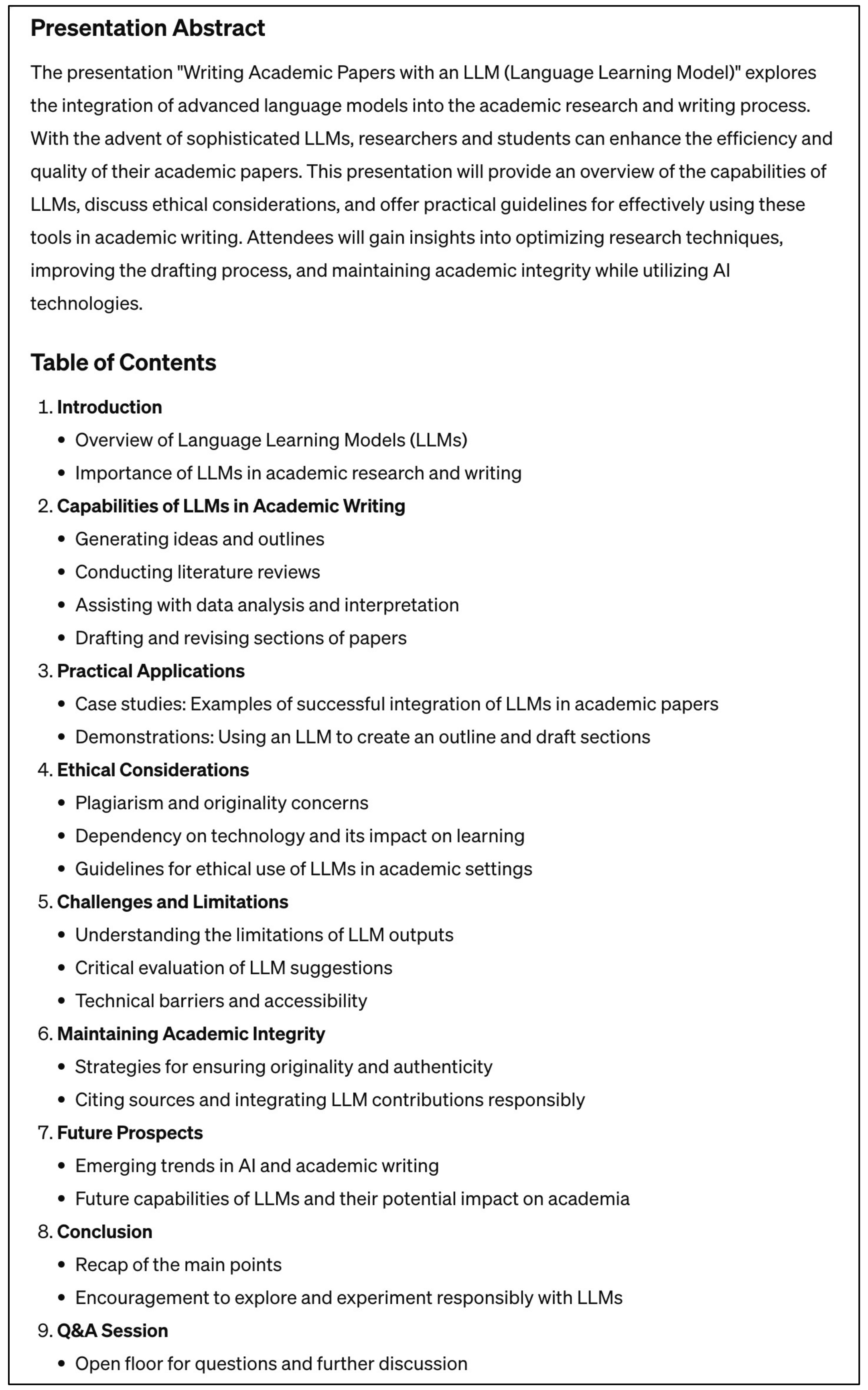
2. **Presentation Outline**: Develop a detailed outline of your presentation. This outline should include:
   - Introduction: Overview of LLMs and their relevance to academic research.
   - Main Body: Section-by-section breakdown, each focusing on different aspects of using LLMs in academic writing (e.g., literature review, data analysis, drafting, and citation).
   - Conclusion: Summary of key points and best practices.

3. **Table of Contents**: Create a table of contents based on the outline. This should list all main sections and sub-sections, indicating the flow and structure of your presentation. Optionally, include estimated time allocations for each section to help manage presentation pacing.

Please ensure that your outline and table of contents provide a clear roadmap for your presentation, reflecting a logical flow and progression of ideas.

TIP 4 : Empower your prompt

기존 프롬프트



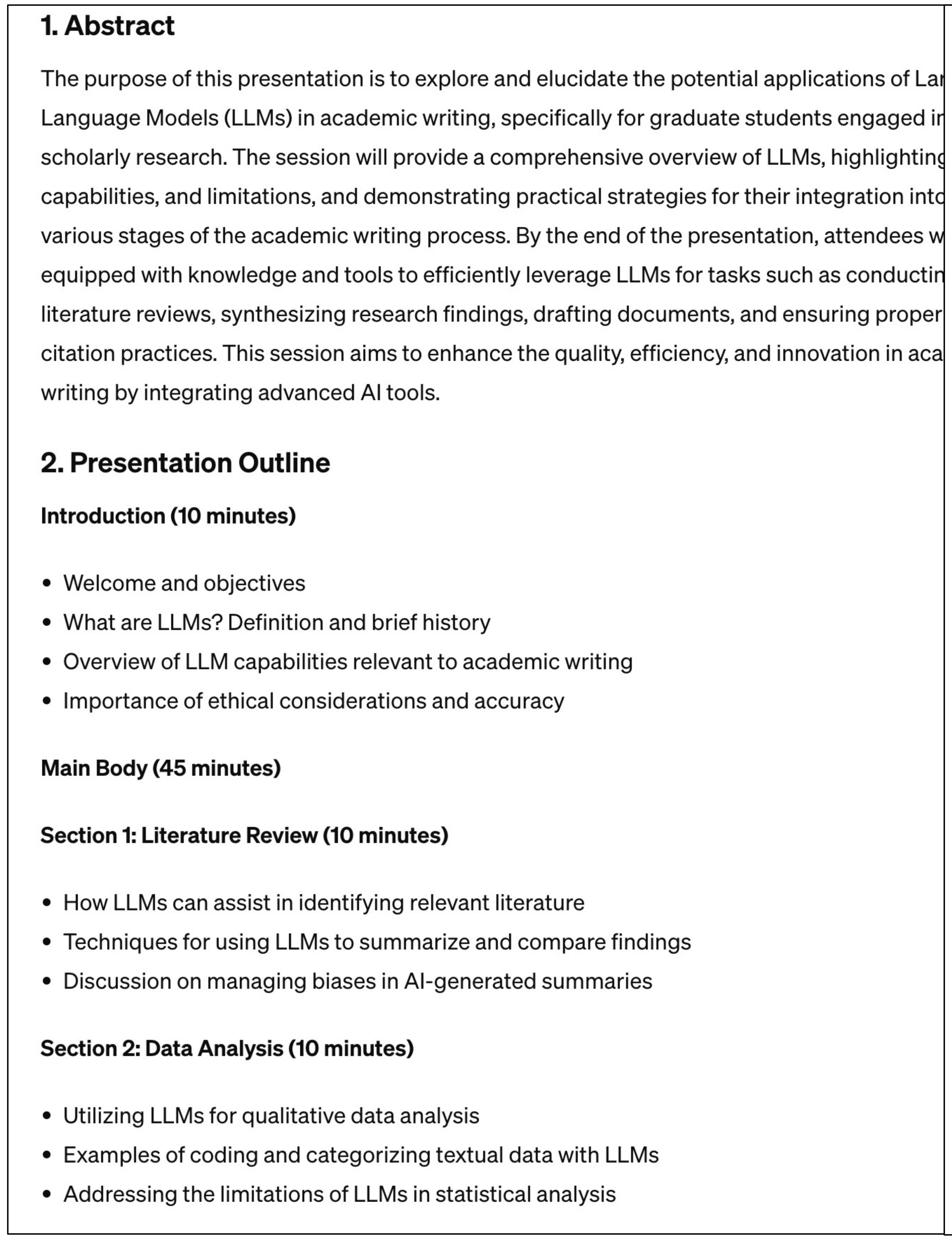
Presentation Abstract

The presentation "Writing Academic Papers with an LLM (Language Learning Model)" explores the integration of advanced language models into the academic research and writing process. With the advent of sophisticated LLMs, researchers and students can enhance the efficiency and quality of their academic papers. This presentation will provide an overview of the capabilities of LLMs, discuss ethical considerations, and offer practical guidelines for effectively using these tools in academic writing. Attendees will gain insights into optimizing research techniques, improving the drafting process, and maintaining academic integrity while utilizing AI technologies.

Table of Contents

1. **Introduction**
   - Overview of Language Learning Models (LLMs)
   - Importance of LLMs in academic research and writing
2. **Capabilities of LLMs in Academic Writing**
   - Generating ideas and outlines
   - Conducting literature reviews
   - Assisting with data analysis and interpretation
   - Drafting and revising sections of papers
3. **Practical Applications**
   - Case studies: Examples of successful integration of LLMs in academic papers
   - Demonstrations: Using an LLM to create an outline and draft sections
4. **Ethical Considerations**
   - Plagiarism and originality concerns
   - Dependency on technology and its impact on learning
   - Guidelines for ethical use of LLMs in academic settings
5. **Challenges and Limitations**
   - Understanding the limitations of LLM outputs
   - Critical evaluation of LLM suggestions
   - Technical barriers and accessibility
6. **Maintaining Academic Integrity**
   - Strategies for ensuring originality and authenticity
   - Citing sources and integrating LLM contributions responsibly
7. **Future Prospects**
   - Emerging trends in AI and academic writing
   - Future capabilities of LLMs and their potential impact on academia
8. **Conclusion**
   - Recap of the main points
   - Encouragement to explore and experiment responsibly with LLMs
9. **Q&A Session**
   - Open floor for questions and further discussion

개선된 프롬프트



1. Abstract

The purpose of this presentation is to explore and elucidate the potential applications of Lar
Language Models (LLMs) in academic writing, specifically for graduate students engaged ir
scholarly research. The session will provide a comprehensive overview of LLMs, highlighting
capabilities, and limitations, and demonstrating practical strategies for their integration intc
various stages of the academic writing process. By the end of the presentation, attendees w
equipped with knowledge and tools to efficiently leverage LLMs for tasks such as conductin
literature reviews, synthesizing research findings, drafting documents, and ensuring proper
citation practices. This session aims to enhance the quality, efficiency, and innovation in aca
writing by integrating advanced AI tools.

2. Presentation Outline

Introduction (10 minutes)

- Welcome and objectives
- What are LLMs? Definition and brief history
- Overview of LLM capabilities relevant to academic writing
- Importance of ethical considerations and accuracy

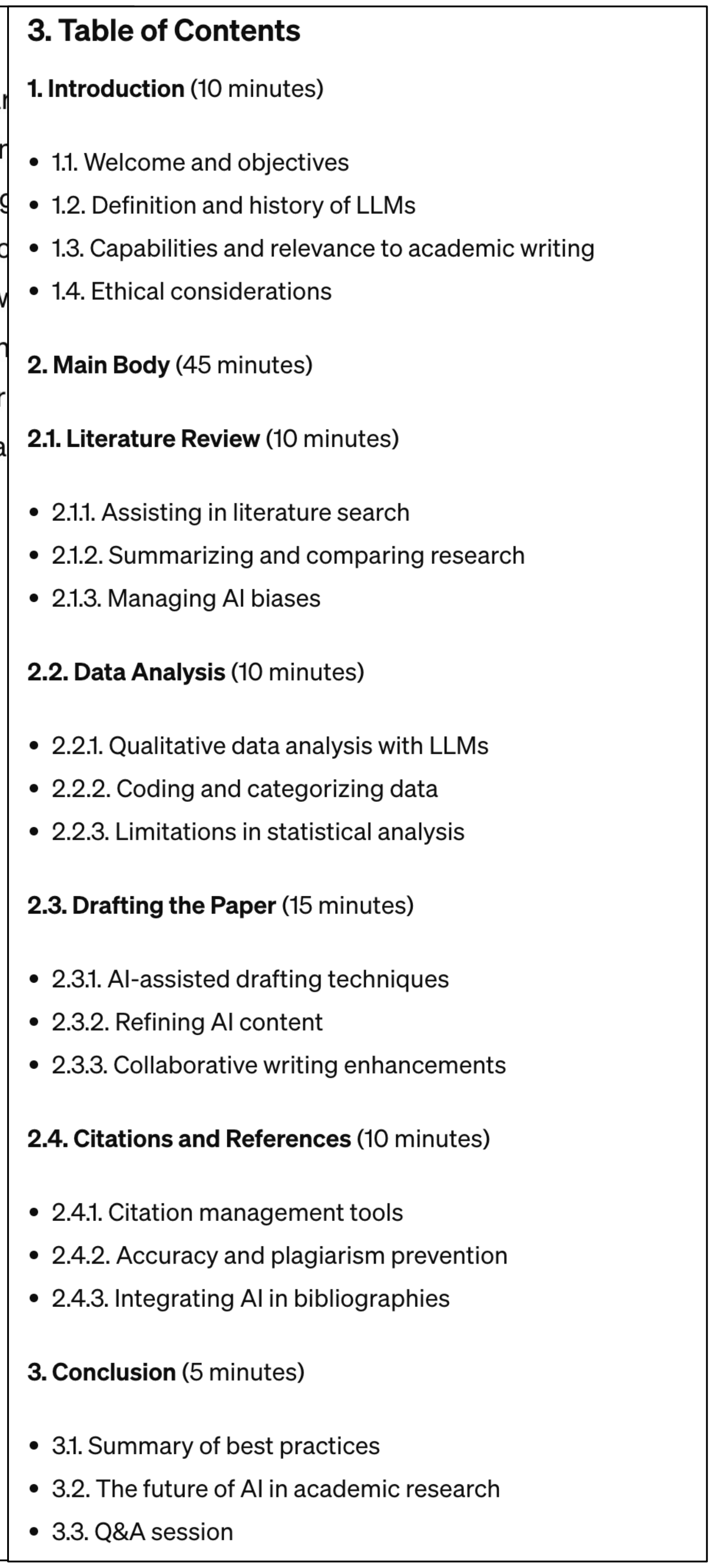
Main Body (45 minutes)

Section 1: Literature Review (10 minutes)

- How LLMs can assist in identifying relevant literature
- Techniques for using LLMs to summarize and compare findings
- Discussion on managing biases in AI-generated summaries

Section 2: Data Analysis (10 minutes)

- Utilizing LLMs for qualitative data analysis
- Examples of coding and categorizing textual data with LLMs
- Addressing the limitations of LLMs in statistical analysis



3. Table of Contents

1. Introduction (10 minutes)

- 1.1. Welcome and objectives
- 1.2. Definition and history of LLMs
- 1.3. Capabilities and relevance to academic writing
- 1.4. Ethical considerations

2. Main Body (45 minutes)

2.1. Literature Review (10 minutes)

- 2.1.1. Assisting in literature search
- 2.1.2. Summarizing and comparing research
- 2.1.3. Managing AI biases

2.2. Data Analysis (10 minutes)

- 2.2.1. Qualitative data analysis with LLMs
- 2.2.2. Coding and categorizing data
- 2.2.3. Limitations in statistical analysis

2.3. Drafting the Paper (15 minutes)

- 2.3.1. AI-assisted drafting techniques
- 2.3.2. Refining AI content
- 2.3.3. Collaborative writing enhancements

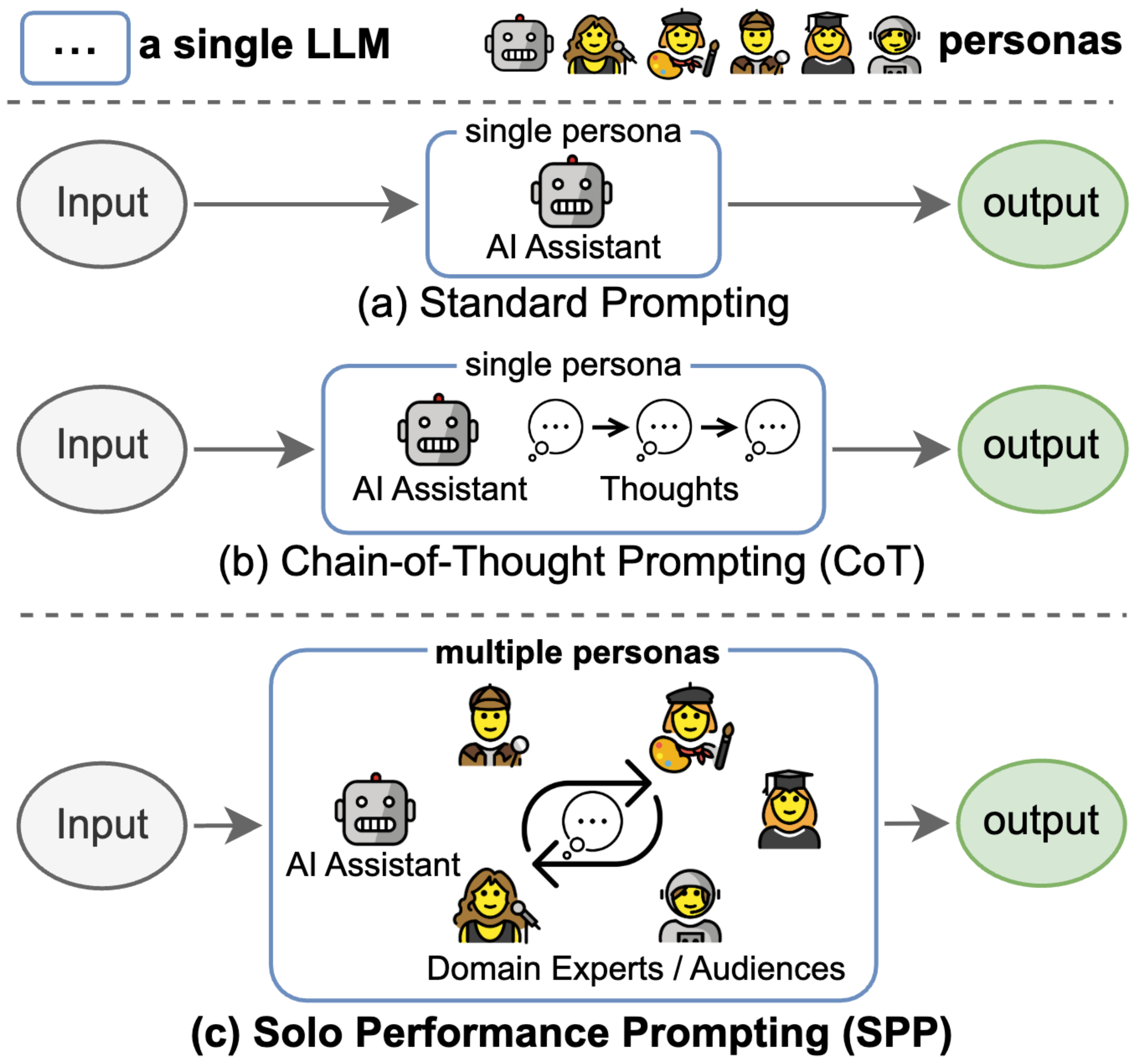
2.4. Citations and References (10 minutes)

- 2.4.1. Citation management tools
- 2.4.2. Accuracy and plagiarism prevention
- 2.4.3. Integrating AI in bibliographies

3. Conclusion (5 minutes)

- 3.1. Summary of best practices
- 3.2. The future of AI in academic research
- 3.3. Q&A session

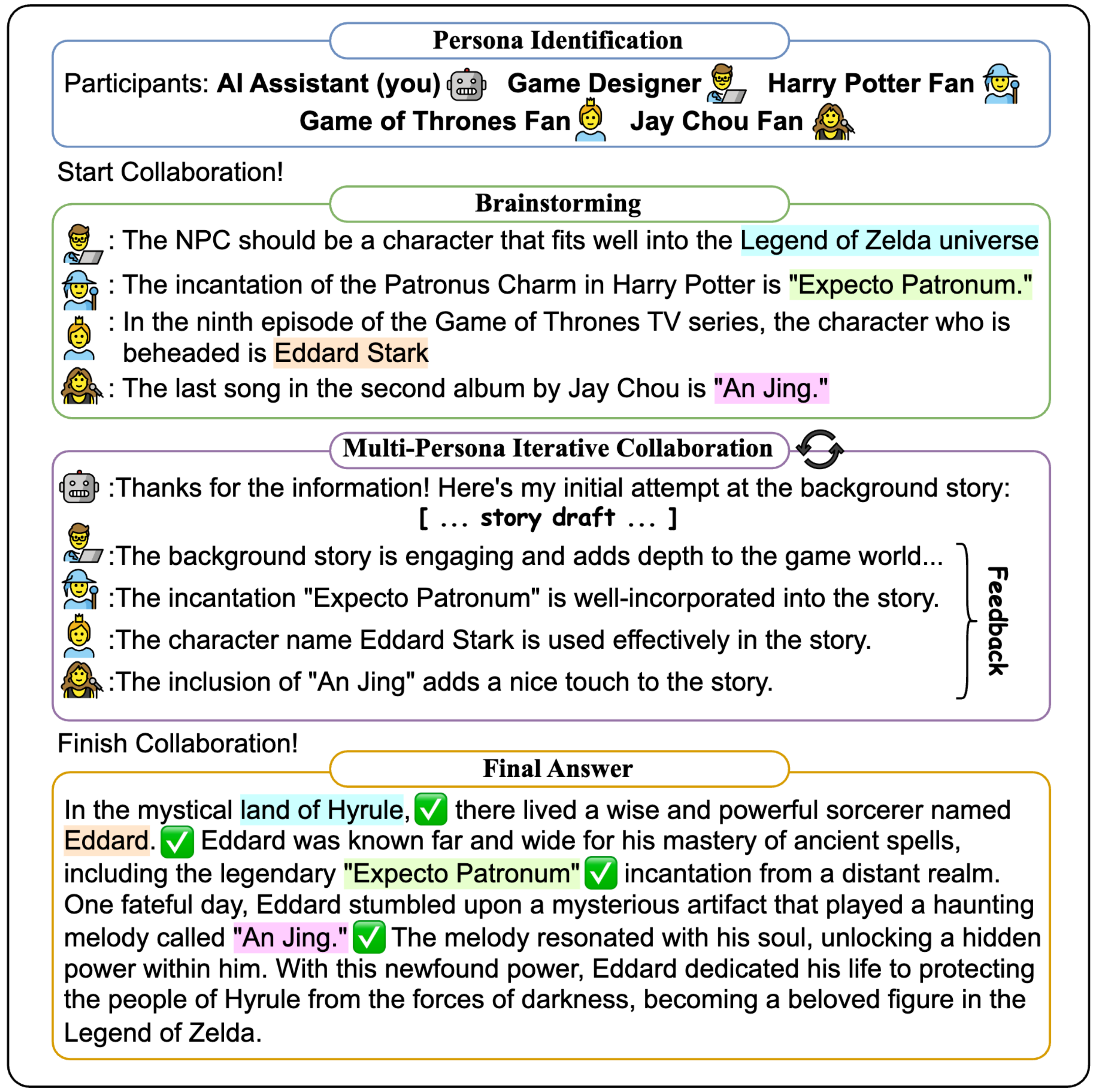
TIP 5 : SPP (Solo Performance Prompting)



(a) Standard Prompting

(b) Chain-of-Thought Prompting (CoT)

(c) Solo Performance Prompting (SPP)



Persona Identification

Participants: **AI Assistant (you)** **Game Designer** **Harry Potter Fan** **Game of Thrones Fan** **Jay Chou Fan**

Start Collaboration!

Brainstorming

: The NPC should be a character that fits well into the Legend of Zelda universe

: The incantation of the Patronus Charm in Harry Potter is "Expecto Patronum."

: In the ninth episode of the Game of Thrones TV series, the character who is beheaded is Eddard Stark

: The last song in the second album by Jay Chou is "An Jing."

Multi-Persona Iterative Collaboration

:Thanks for the information! Here's my initial attempt at the background story:

`[ ... story draft ... ]`

:The background story is engaging and adds depth to the game world...

:The incantation "Expecto Patronum" is well-incorporated into the story.

:The character name Eddard Stark is used effectively in the story.

:The inclusion of "An Jing" adds a nice touch to the story.

Finish Collaboration!

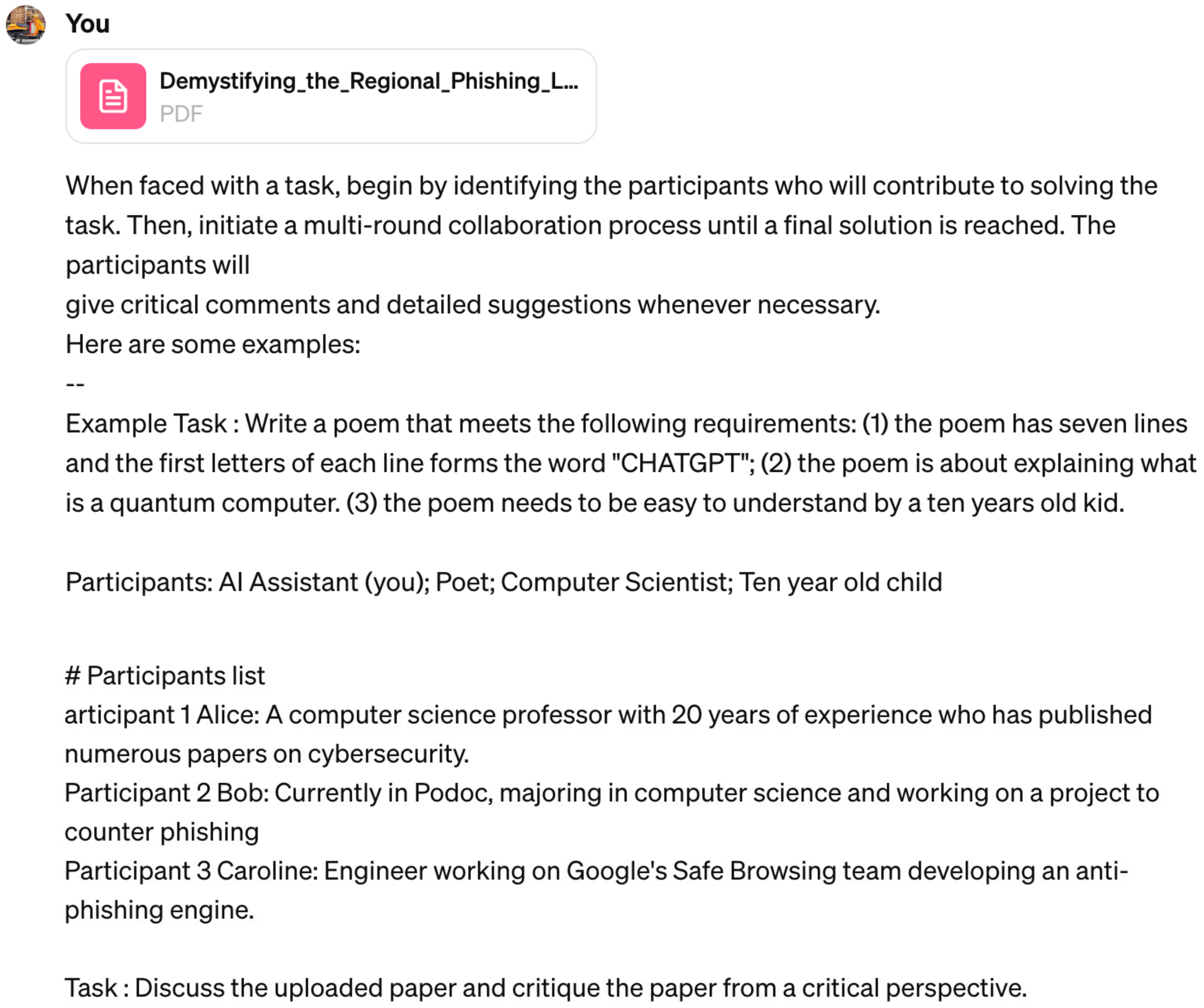
Final Answer

In the mystical land of Hyrule, ✅ there lived a wise and powerful sorcerer named Eddard. ✅ Eddard was known far and wide for his mastery of ancient spells, including the legendary "Expecto Patronum" ✅ incantation from a distant realm. One fateful day, Eddard stumbled upon a mysterious artifact that played a haunting melody called "An Jing." ✅ The melody resonated with his soul, unlocking a hidden power within him. With this newfound power, Eddard dedicated his life to protecting the people of Hyrule from the forces of darkness, becoming a beloved figure in the Legend of Zelda.

Solo Performance Prompting Result (GPT-4)

출처 : https://arxiv.org/abs/2307.05300

TIP 5 : SPP (Solo Performance Prompting)



You

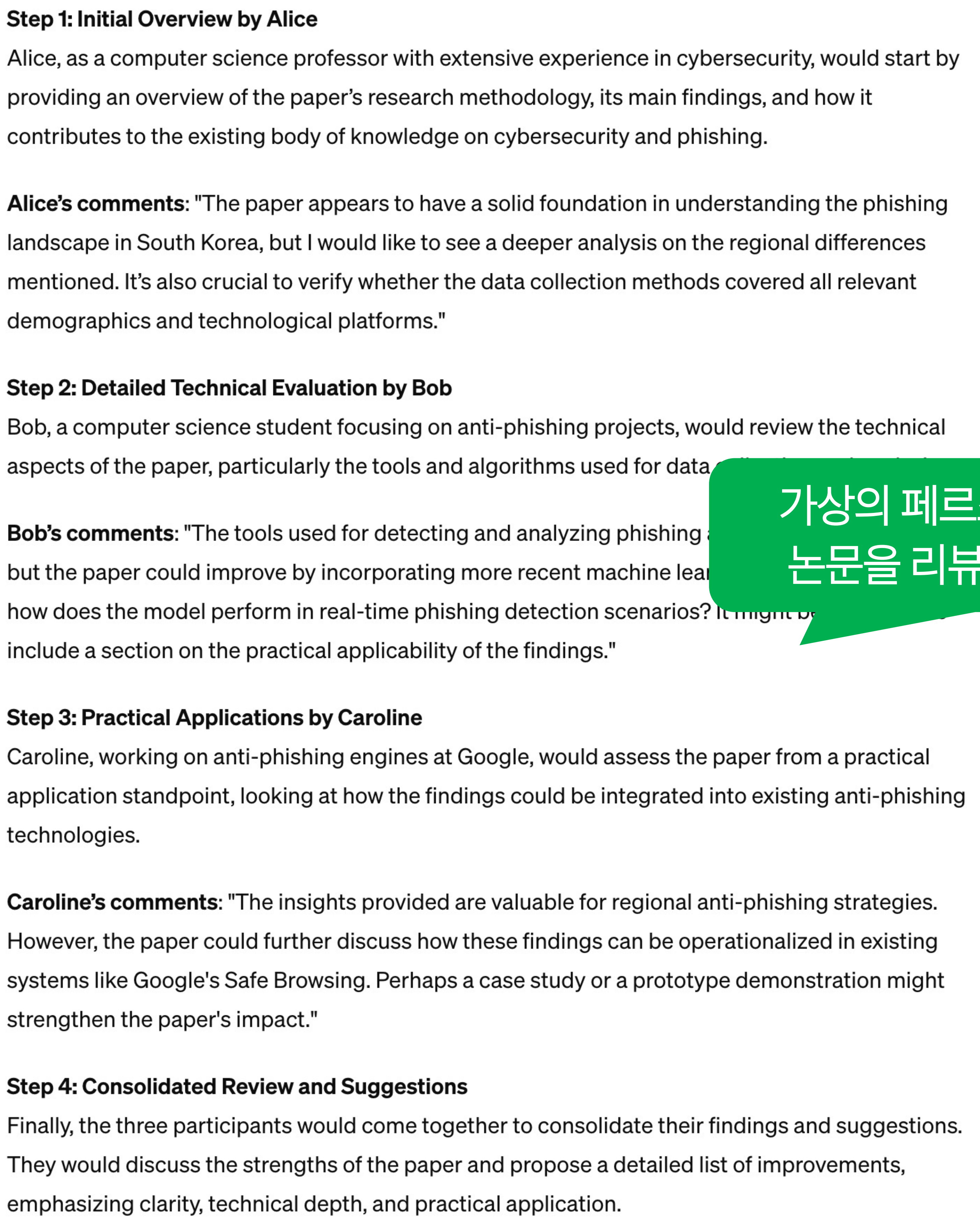
Demystifying_the_Regional_Phishing_L...
PDF

When faced with a task, begin by identifying the participants who will contribute to solving the task. Then, initiate a multi-round collaboration process until a final solution is reached. The participants will
give critical comments and detailed suggestions whenever necessary.
Here are some examples:
--
Example Task : Write a poem that meets the following requirements: (1) the poem has seven lines and the first letters of each line forms the word "CHATGPT"; (2) the poem is about explaining what is a quantum computer. (3) the poem needs to be easy to understand by a ten years old kid.

Participants: AI Assistant (you); Poet; Computer Scientist; Ten year old child

Participants list
articipant 1 Alice: A computer science professor with 20 years of experience who has published numerous papers on cybersecurity.
Participant 2 Bob: Currently in Podoc, majoring in computer science and working on a project to counter phishing
Participant 3 Caroline: Engineer working on Google's Safe Browsing team developing an anti-phishing engine.

Task : Discuss the uploaded paper and critique the paper from a critical perspective.



Step 1: Initial Overview by Alice
Alice, as a computer science professor with extensive experience in cybersecurity, would start by providing an overview of the paper's research methodology, its main findings, and how it contributes to the existing body of knowledge on cybersecurity and phishing.

Alice's comments: "The paper appears to have a solid foundation in understanding the phishing landscape in South Korea, but I would like to see a deeper analysis on the regional differences mentioned. It's also crucial to verify whether the data collection methods covered all relevant demographics and technological platforms."

Step 2: Detailed Technical Evaluation by Bob
Bob, a computer science student focusing on anti-phishing projects, would review the technical aspects of the paper, particularly the tools and algorithms used for data

Bob's comments: "The tools used for detecting and analyzing phishing
but the paper could improve by incorporating more recent machine lea
how does the model perform in real-time phishing detection scenarios? It might
include a section on the practical applicability of the findings."

Step 3: Practical Applications by Caroline
Caroline, working on anti-phishing engines at Google, would assess the paper from a practical application standpoint, looking at how the findings could be integrated into existing anti-phishing technologies.

Caroline's comments: "The insights provided are valuable for regional anti-phishing strategies. However, the paper could further discuss how these findings can be operationalized in existing systems like Google's Safe Browsing. Perhaps a case study or a prototype demonstration might strengthen the paper's impact."

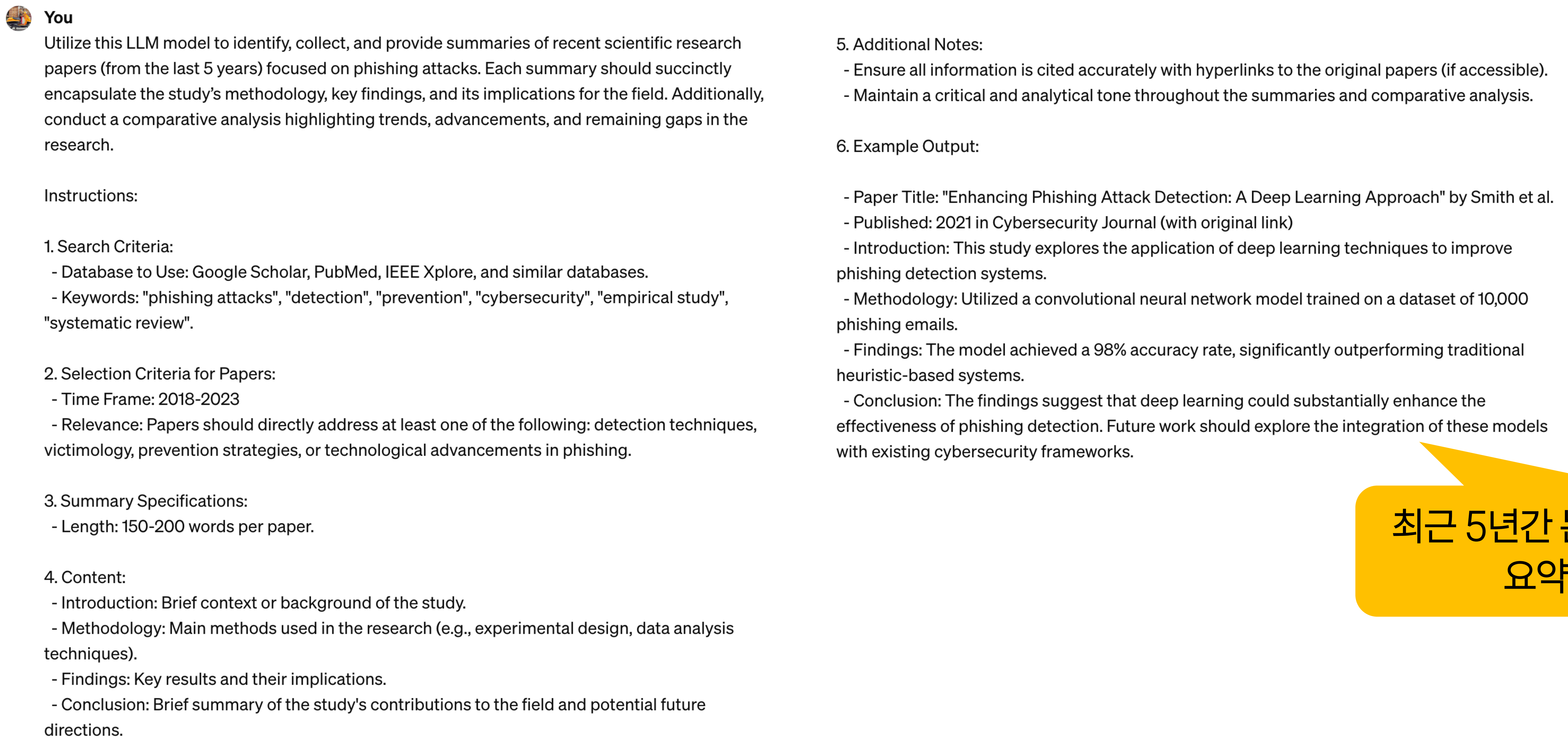
Step 4: Consolidated Review and Suggestions
Finally, the three participants would come together to consolidate their findings and suggestions. They would discuss the strengths of the paper and propose a detailed list of improvements, emphasizing clarity, technical depth, and practical application.

가상의 페르소나 교수님(?)이
논문을 리뷰하고 피드백 제공

Academic Writing with LLM

Literature Search & Review

chatGPT4나 Gemini를 이용해서 논문 수집과 요약을 자동화 할 수 있지 않을까? (With Internet Browsing)



You

Utilize this LLM model to identify, collect, and provide summaries of recent scientific research papers (from the last 5 years) focused on phishing attacks. Each summary should succinctly encapsulate the study's methodology, key findings, and its implications for the field. Additionally, conduct a comparative analysis highlighting trends, advancements, and remaining gaps in the research.

Instructions:

1. Search Criteria:
 - Database to Use: Google Scholar, PubMed, IEEE Xplore, and similar databases.
 - Keywords: "phishing attacks", "detection", "prevention", "cybersecurity", "empirical study", "systematic review".

2. Selection Criteria for Papers:
 - Time Frame: 2018-2023
 - Relevance: Papers should directly address at least one of the following: detection techniques, victimology, prevention strategies, or technological advancements in phishing.

3. Summary Specifications:
 - Length: 150-200 words per paper.

4. Content:
 - Introduction: Brief context or background of the study.
 - Methodology: Main methods used in the research (e.g., experimental design, data analysis techniques).
 - Findings: Key results and their implications.
 - Conclusion: Brief summary of the study's contributions to the field and potential future directions.

5. Additional Notes:
 - Ensure all information is cited accurately with hyperlinks to the original papers (if accessible).
 - Maintain a critical and analytical tone throughout the summaries and comparative analysis.

6. Example Output:

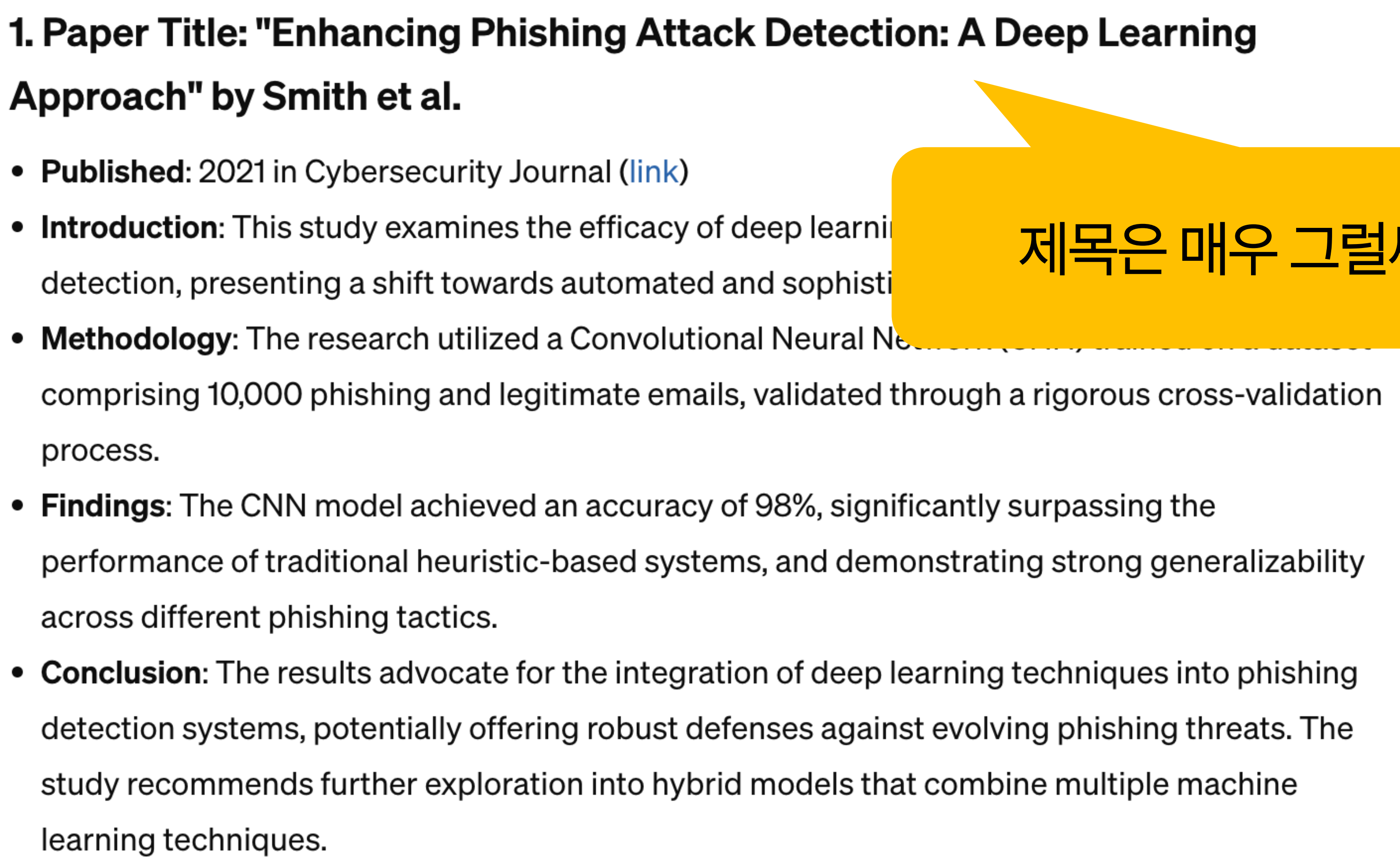
 - Paper Title: "Enhancing Phishing Attack Detection: A Deep Learning Approach" by Smith et al.
 - Published: 2021 in Cybersecurity Journal (with original link)
 - Introduction: This study explores the application of deep learning techniques to improve phishing detection systems.
 - Methodology: Utilized a convolutional neural network model trained on a dataset of 10,000 phishing emails.
 - Findings: The model achieved a 98% accuracy rate, significantly outperforming traditional heuristic-based systems.
 - Conclusion: The findings suggest that deep learning could substantially enhance the effectiveness of phishing detection. Future work should explore the integration of these models with existing cybersecurity frameworks.

최근 5년간 논문을 수집해서 포맷에 맞게
요약/정리 해달라는 요청

Literature Search & Review

chatGPT4나 Gemini를 이용해서 논문 수집과 요약을 자동화 할 수 있지 않을까?

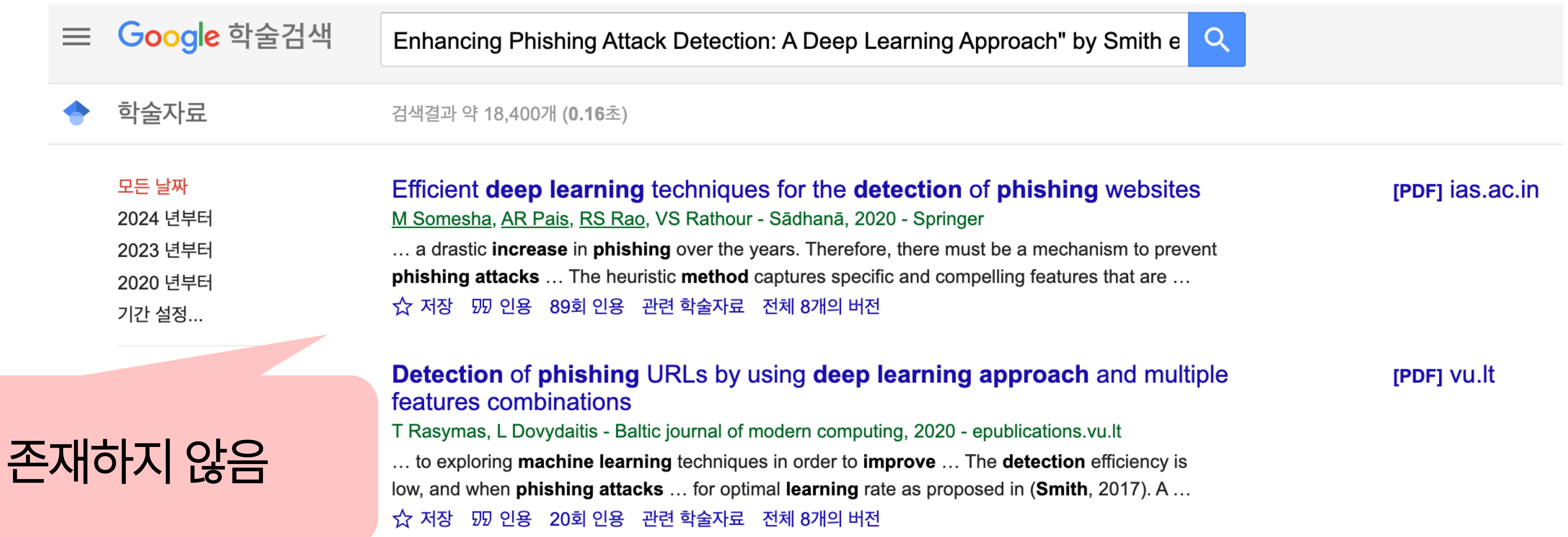
네… 안됩니다. (할루시네이션 Party)



1. Paper Title: "Enhancing Phishing Attack Detection: A Deep Learning Approach" by Smith et al.

- **Published**: 2021 in Cybersecurity Journal (link)
- **Introduction**: This study examines the efficacy of deep learni
detection, presenting a shift towards automated and sophisti
- **Methodology**: The research utilized a Convolutional Neural Ne
comprising 10,000 phishing and legitimate emails, validated through a rigorous cross-validation process.
- **Findings**: The CNN model achieved an accuracy of 98%, significantly surpassing the performance of traditional heuristic-based systems, and demonstrating strong generalizability across different phishing tactics.
- **Conclusion**: The results advocate for the integration of deep learning techniques into phishing detection systems, potentially offering robust defenses against evolving phishing threats. The study recommends further exploration into hybrid models that combine multiple machine learning techniques.

제목은 매우 그럴싸 한데…



Enhancing Phishing Attack Detection: A Deep Learning Approach" by Smith e

검색결과 약 18,400개 (**0.16**초)

Efficient **deep learning** techniques for the **detection** of **phishing** websites — [PDF] ias.ac.in
M Somesha, AR Pais, RS Rao, VS Rathour - Sādhanā, 2020 - Springer
… a drastic **increase** in **phishing** over the years. Therefore, there must be a mechanism to prevent **phishing attacks** … The heuristic **method** captures specific and compelling features that are …
☆ 저장 99 인용 89회 인용 관련 학술자료 전체 8개의 버전

Detection of **phishing** URLs by using **deep learning approach** and multiple features combinations — [PDF] vu.lt
T Rasymas, L Dovydaitis - Baltic journal of modern computing, 2020 - epublications.vu.lt
… to exploring **machine learning** techniques in order to **improve** … The **detection** efficiency is low, and when **phishing attacks** … for optimal **learning** rate as proposed in (**Smith**, 2017). A …
☆ 저장 99 인용 20회 인용 관련 학술자료 전체 8개의 버전

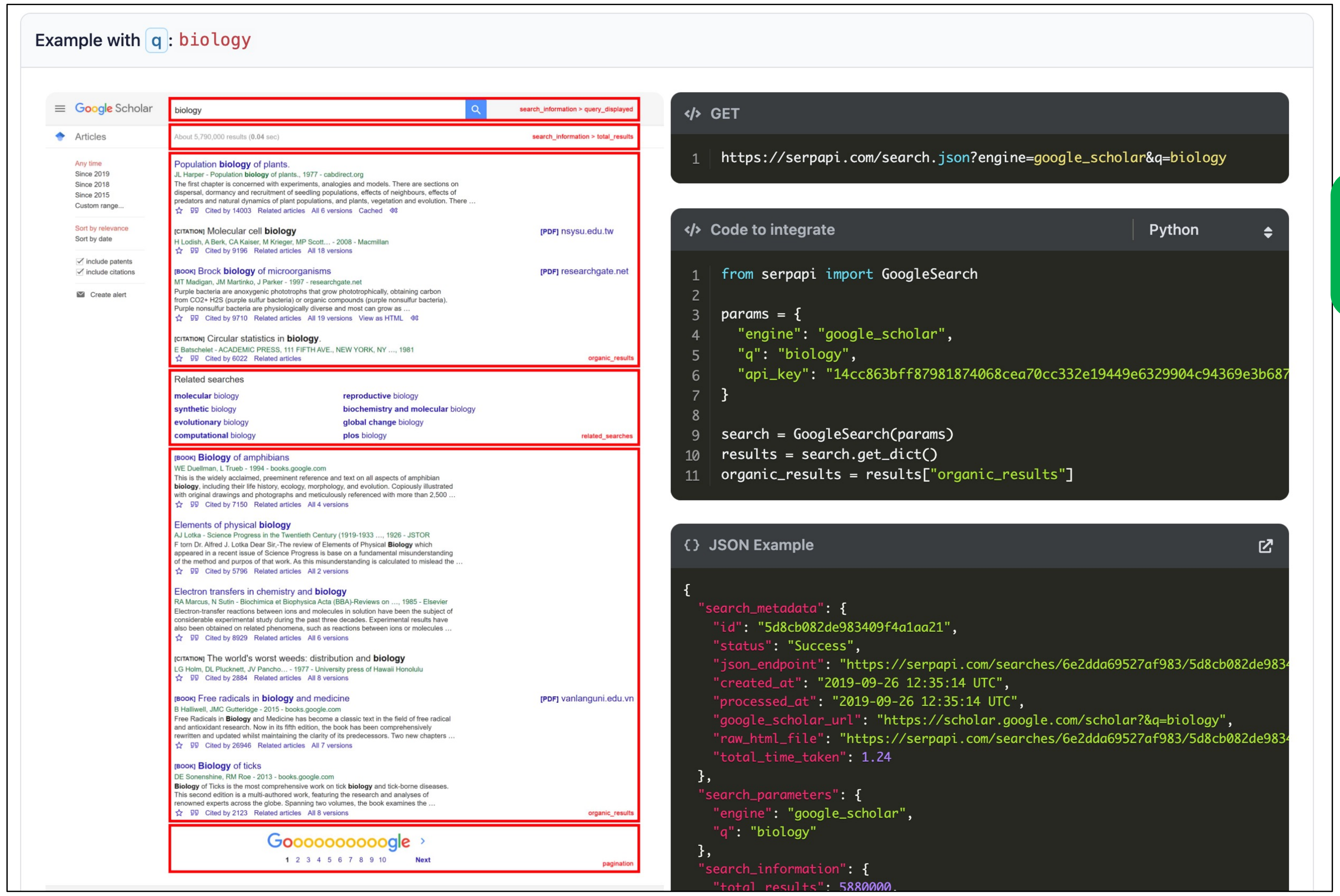
그런 논문은 존재하지 않음

chatGPT / MS Copilot / Gemini 모두 할루시네이션 발생하였으며, 신뢰도 매우 낮음
특히 Gemini는 내일까지 Google Docs로 정리해서 이메일로 보내준다는 희망 고문을 함 (거짓말이었음)

Literature Search & Review

chatGPT4나 Gemini를 이용해서 논문 수집과 요약을 자동화 할 수 있지 않을까?

우리는 결국 방법을 찾을 것이다..



```
https://serpapi.com/search.json?engine=google_scholar&q=biology
```

```python
from serpapi import GoogleSearch

params = {
  "engine": "google_scholar",
  "q": "biology",
  "api_key": "14cc863bff87981874068cea70cc332e19449e6329904c94369e3b687
}

search = GoogleSearch(params)
results = search.get_dict()
organic_results = results["organic_results"]
```

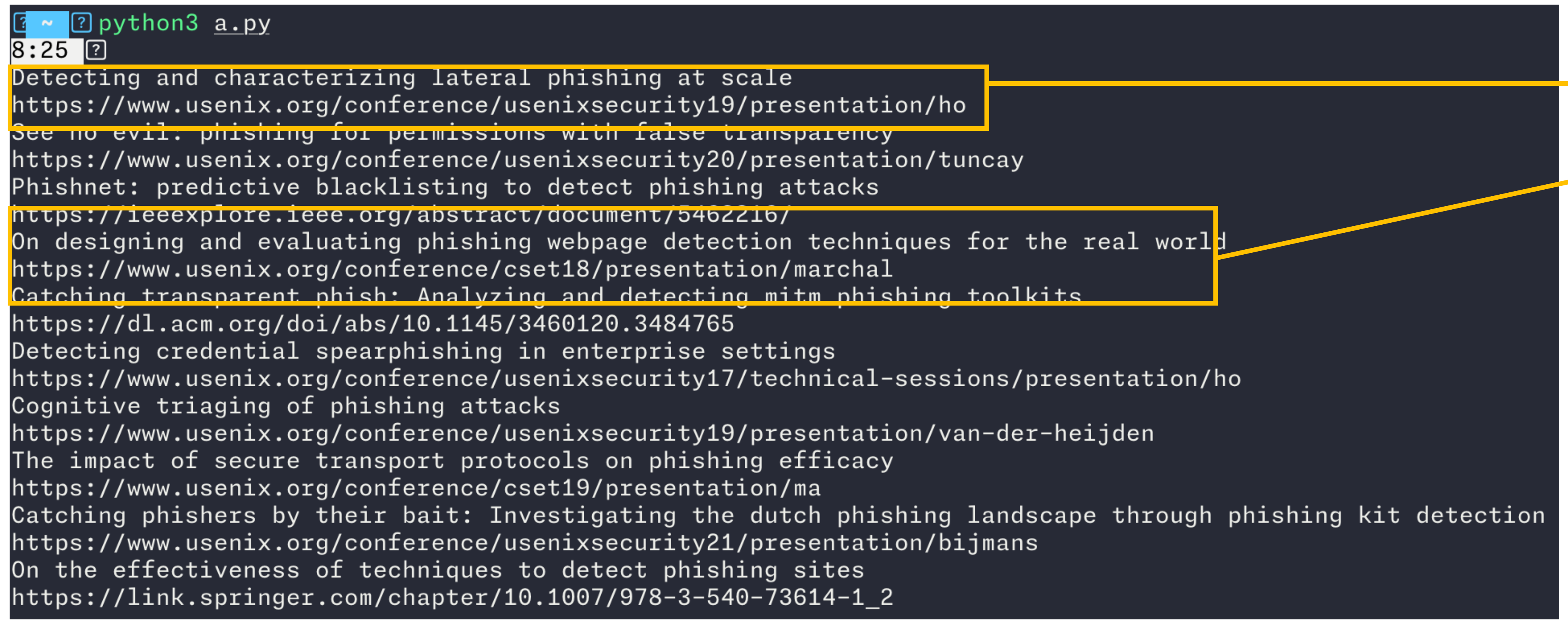
```json
{
  "search_metadata": {
    "id": "5d8cb082de983409f4a1aa21",
    "status": "Success",
    "json_endpoint": "https://serpapi.com/searches/6e2dda69527af983/5d8cb082de983
    "created_at": "2019-09-26 12:35:14 UTC",
    "processed_at": "2019-09-26 12:35:14 UTC",
    "google_scholar_url": "https://scholar.google.com/scholar?&q=biology",
    "raw_html_file": "https://serpapi.com/searches/6e2dda69527af983/5d8cb082de983
    "total_time_taken": 1.24
  },
  "search_parameters": {
    "engine": "google_scholar",
    "q": "biology"
  },
  "search_information": {
    "total_results": 5880000,
```

Google Scholar API from serpapi

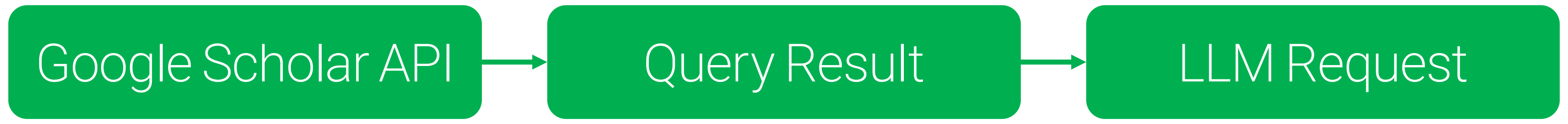
Literature Search & Review

chatGPT4나 Gemini를 이용해서 논문 수집과 요약을 자동화 할 수 있지 않을까?

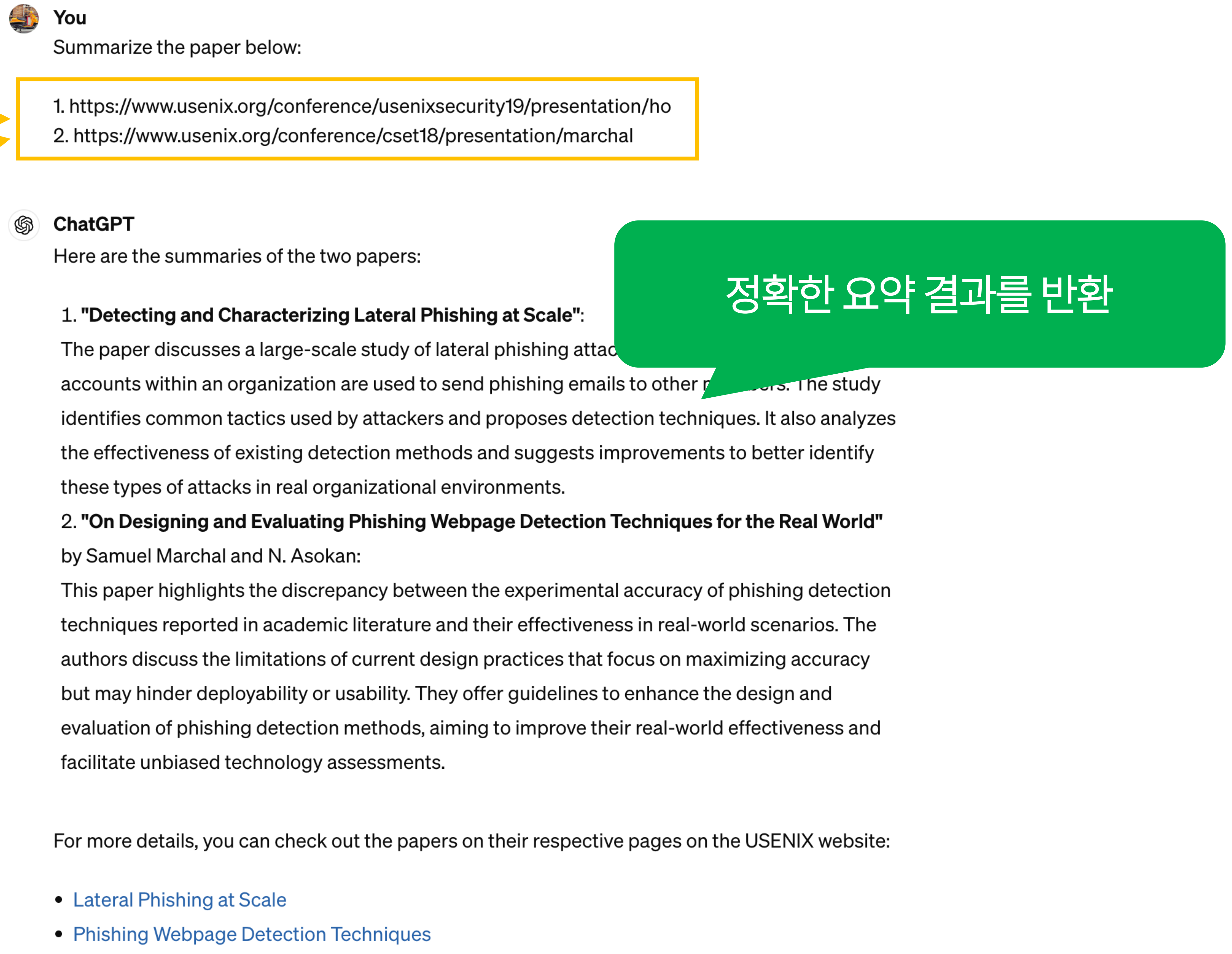
우리는 결국 방법을 찾을 것이다..



```
? ~ ? python3 a.py
8:25 ?
Detecting and characterizing lateral phishing at scale
https://www.usenix.org/conference/usenixsecurity19/presentation/ho
See no evil: phishing for permissions with false transparency
https://www.usenix.org/conference/usenixsecurity20/presentation/tuncay
Phishnet: predictive blacklisting to detect phishing attacks
https://ieeexplore.ieee.org/abstract/document/5462216/
On designing and evaluating phishing webpage detection techniques for the real world
https://www.usenix.org/conference/cset18/presentation/marchal
Catching transparent phish: Analyzing and detecting mitm phishing toolkits
https://dl.acm.org/doi/abs/10.1145/3460120.3484765
Detecting credential spearphishing in enterprise settings
https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/ho
Cognitive triaging of phishing attacks
https://www.usenix.org/conference/usenixsecurity19/presentation/van-der-heijden
The impact of secure transport protocols on phishing efficacy
https://www.usenix.org/conference/cset19/presentation/ma
Catching phishers by their bait: Investigating the dutch phishing landscape through phishing kit detection
https://www.usenix.org/conference/usenixsecurity21/presentation/bijmans
On the effectiveness of techniques to detect phishing sites
https://link.springer.com/chapter/10.1007/978-3-540-73614-1_2
```



Google Scholar API → Query Result → LLM Request



You

Summarize the paper below:

1. https://www.usenix.org/conference/usenixsecurity19/presentation/ho
2. https://www.usenix.org/conference/cset18/presentation/marchal

ChatGPT

Here are the summaries of the two papers:

1. **"Detecting and Characterizing Lateral Phishing at Scale"**:
   The paper discusses a large-scale study of lateral phishing attac accounts within an organization are used to send phishing emails to other r ers. The study identifies common tactics used by attackers and proposes detection techniques. It also analyzes the effectiveness of existing detection methods and suggests improvements to better identify these types of attacks in real organizational environments.
2. **"On Designing and Evaluating Phishing Webpage Detection Techniques for the Real World"** by Samuel Marchal and N. Asokan:
   This paper highlights the discrepancy between the experimental accuracy of phishing detection techniques reported in academic literature and their effectiveness in real-world scenarios. The authors discuss the limitations of current design practices that focus on maximizing accuracy but may hinder deployability or usability. They offer guidelines to enhance the design and evaluation of phishing detection methods, aiming to improve their real-world effectiveness and facilitate unbiased technology assessments.

For more details, you can check out the papers on their respective pages on the USENIX website:

- Lateral Phishing at Scale
- Phishing Webpage Detection Techniques

정확한 요약 결과를 반환

Finding Research Topics from Papers

기존 논문을 분석하여 Gap(보완이 필요한 부분)과 추가 연구 주제를 제안

Prompt

Based on the comprehensive review provided in the selected research paper, identify gaps in the current literature and suggest potential future research topics. Use the following guidelines to aid your analysis:

1. **Gap Identification**:
  - Review the discussion and conclusion sections of the paper for any limitations acknowledged by the authors.
  - Consider areas where the authors call for further research or where findings are inconclusive.
  - Examine whether there are emerging trends or recent technologies not covered by the paper.

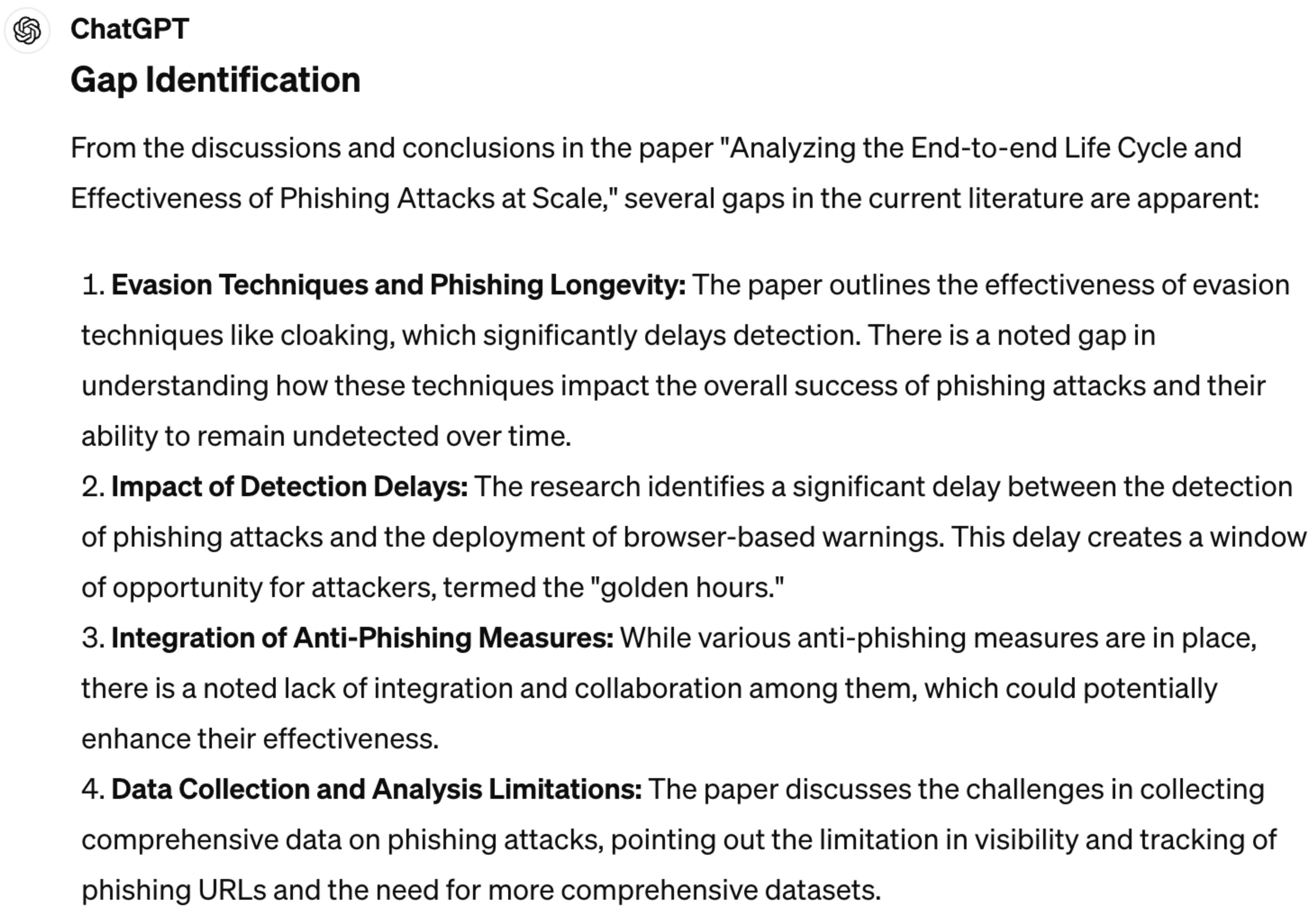
2. **Future Research Suggestions**:
  - For each identified gap, propose a research question or topic that could address this void.
  - Suggest methodologies or theoretical frameworks that could be used to explore these topics.
  - Consider the potential impact of the research, such as advancements in knowledge, technology, or societal benefits.

3. **Output Format**:
  - Provide your findings in a structured format:
    - **Literature Gaps:** List key gaps identified.
    - **Research Suggestions:** For each gap, detail a potential research topic, including possible methods and impacts.

Ensure that your analysis is critical and thorough, providing a clear pathway from identified gaps to future research possibilities.

Finding Research Topics from Papers

기존 논문을 분석하여 Gap(보완이 필요한 부분)과 추가 연구 주제를 제안

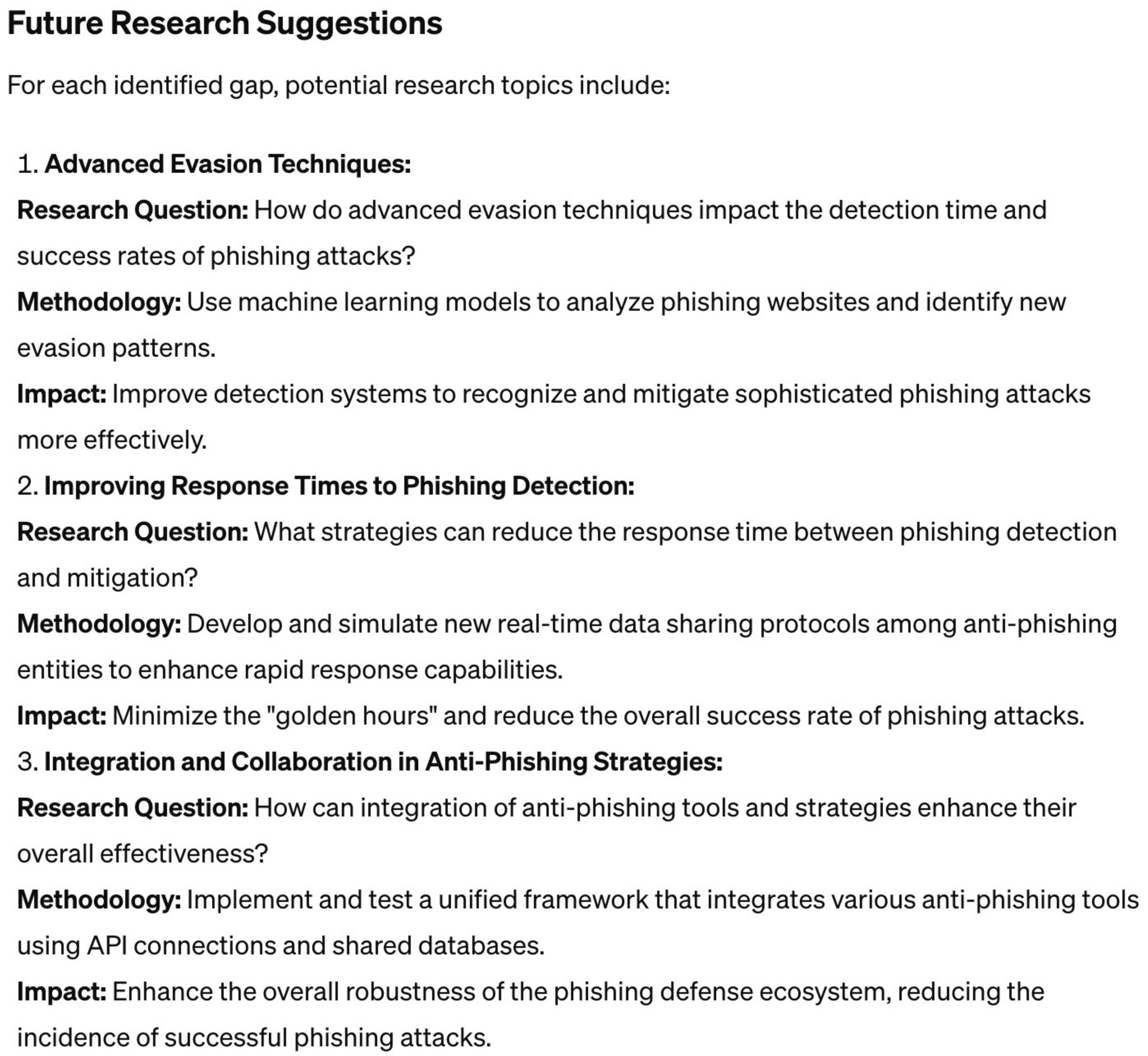


ChatGPT

Gap Identification

From the discussions and conclusions in the paper "Analyzing the End-to-end Life Cycle and Effectiveness of Phishing Attacks at Scale," several gaps in the current literature are apparent:

1. **Evasion Techniques and Phishing Longevity:** The paper outlines the effectiveness of evasion techniques like cloaking, which significantly delays detection. There is a noted gap in understanding how these techniques impact the overall success of phishing attacks and their ability to remain undetected over time.
2. **Impact of Detection Delays:** The research identifies a significant delay between the detection of phishing attacks and the deployment of browser-based warnings. This delay creates a window of opportunity for attackers, termed the "golden hours."
3. **Integration of Anti-Phishing Measures:** While various anti-phishing measures are in place, there is a noted lack of integration and collaboration among them, which could potentially enhance their effectiveness.
4. **Data Collection and Analysis Limitations:** The paper discusses the challenges in collecting comprehensive data on phishing attacks, pointing out the limitation in visibility and tracking of phishing URLs and the need for more comprehensive datasets.



Future Research Suggestions

For each identified gap, potential research topics include:

1. **Advanced Evasion Techniques:**

Research Question: How do advanced evasion techniques impact the detection time and success rates of phishing attacks?

Methodology: Use machine learning models to analyze phishing websites and identify new evasion patterns.

Impact: Improve detection systems to recognize and mitigate sophisticated phishing attacks more effectively.

2. **Improving Response Times to Phishing Detection:**

Research Question: What strategies can reduce the response time between phishing detection and mitigation?

Methodology: Develop and simulate new real-time data sharing protocols among anti-phishing entities to enhance rapid response capabilities.

Impact: Minimize the "golden hours" and reduce the overall success rate of phishing attacks.

3. **Integration and Collaboration in Anti-Phishing Strategies:**

Research Question: How can integration of anti-phishing tools and strategies enhance their overall effectiveness?

Methodology: Implement and test a unified framework that integrates various anti-phishing tools using API connections and shared databases.

Impact: Enhance the overall robustness of the phishing defense ecosystem, reducing the incidence of successful phishing attacks.

Finding Research Topics from Papers

LLM이 제안한 논문의 Gap으로 부터 예상 가능한 질문 목록 뽑기

Prompt

You have completed a literature review on [specific topic]. Based on this review, identify areas where current research is lacking or presents conflicting information.

1. **Summary of Identified Gaps**: Briefly summarize the key gaps you have identified in the literature. These might include areas with minimal research, emerging trends, or ongoing debates among scholars.

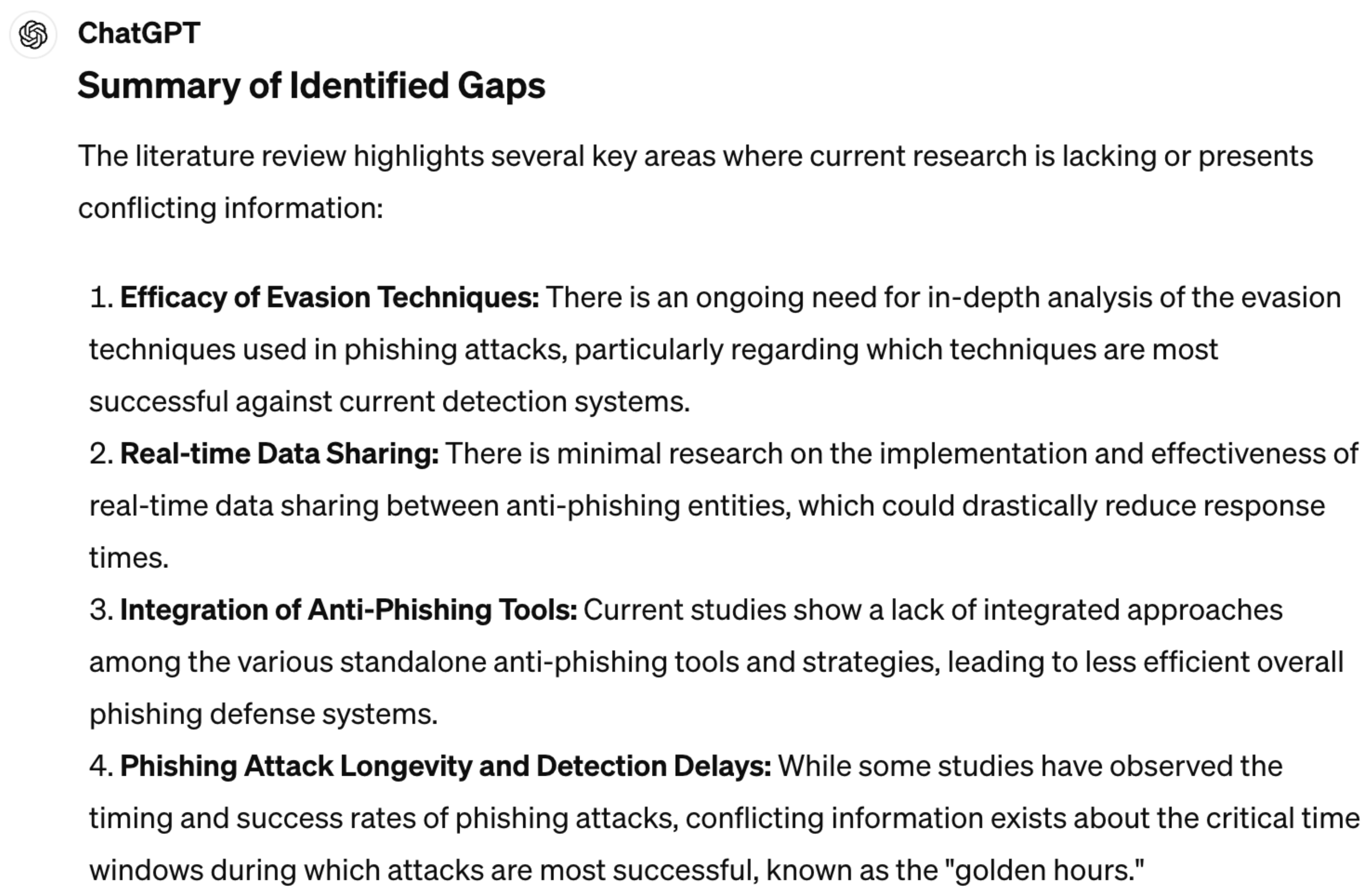
2. **Formulating Research Questions**: Propose potential research questions that address these gaps. Ensure that your questions are:
   - Specific: Clearly define the aspect of the topic you wish to explore.
   - Relevant: Connect directly to the gaps identified and are significant to the field.
   - Feasible: Consider the practicality of answering these questions with available methods and resources.

3. **Examples and Guidance**:
   - If the gap is a lack of research on a particular aspect, a question might be: "How does [variable] affect [outcome] in [context]?"
   - If there is conflicting evidence, consider: "What are the causes of differing outcomes in studies of [topic]?"

Please provide a list of at least three research questions that could guide future studies in this area.

Finding Research Topics from Papers

LLM이 제안한 논문의 Gap으로 부터 예상 가능한 질문 목록 뽑기

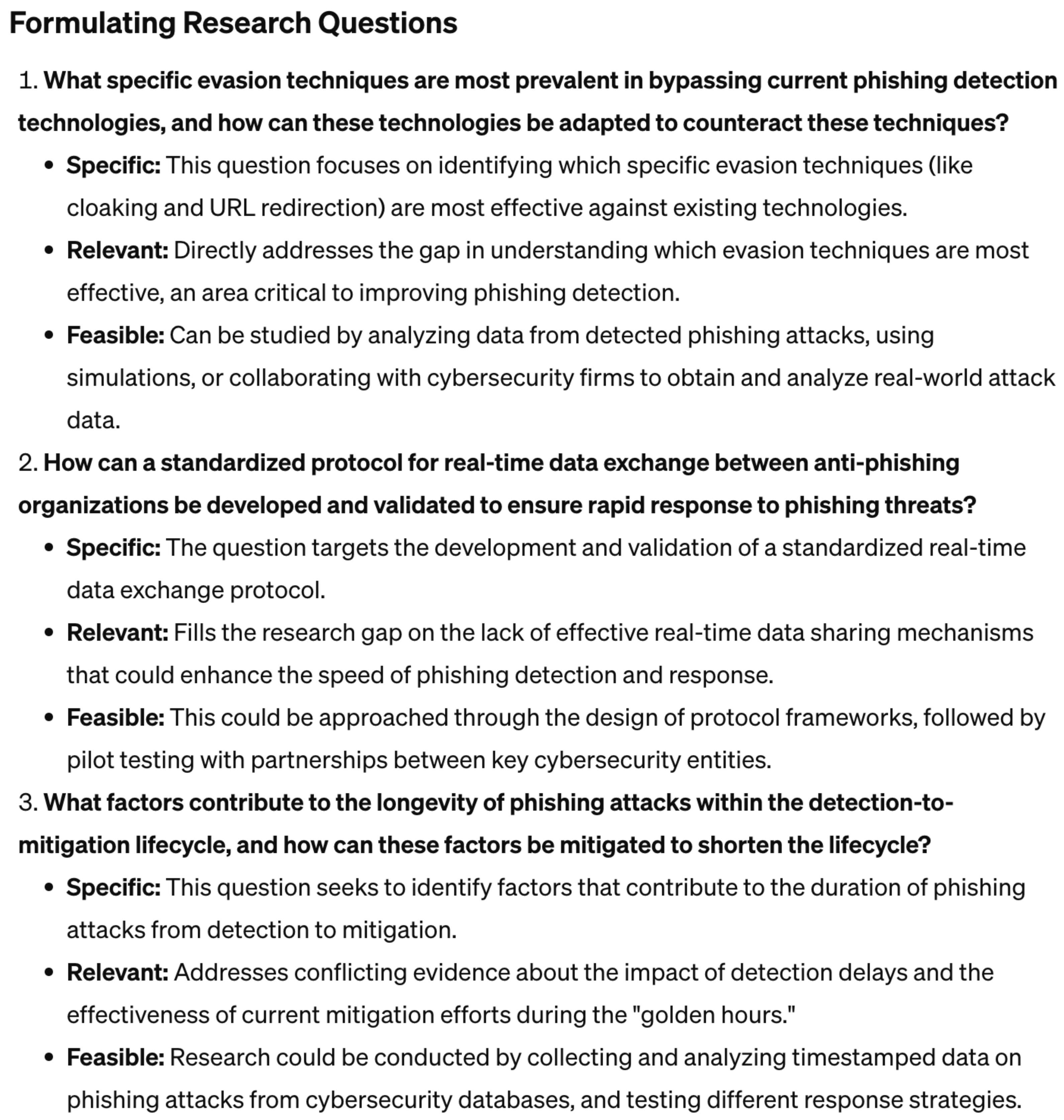


ChatGPT

Summary of Identified Gaps

The literature review highlights several key areas where current research is lacking or presents conflicting information:

1. **Efficacy of Evasion Techniques:** There is an ongoing need for in-depth analysis of the evasion techniques used in phishing attacks, particularly regarding which techniques are most successful against current detection systems.
2. **Real-time Data Sharing:** There is minimal research on the implementation and effectiveness of real-time data sharing between anti-phishing entities, which could drastically reduce response times.
3. **Integration of Anti-Phishing Tools:** Current studies show a lack of integrated approaches among the various standalone anti-phishing tools and strategies, leading to less efficient overall phishing defense systems.
4. **Phishing Attack Longevity and Detection Delays:** While some studies have observed the timing and success rates of phishing attacks, conflicting information exists about the critical time windows during which attacks are most successful, known as the "golden hours."



Formulating Research Questions

1. **What specific evasion techniques are most prevalent in bypassing current phishing detection technologies, and how can these technologies be adapted to counteract these techniques?**
   - **Specific:** This question focuses on identifying which specific evasion techniques (like cloaking and URL redirection) are most effective against existing technologies.
   - **Relevant:** Directly addresses the gap in understanding which evasion techniques are most effective, an area critical to improving phishing detection.
   - **Feasible:** Can be studied by analyzing data from detected phishing attacks, using simulations, or collaborating with cybersecurity firms to obtain and analyze real-world attack data.
2. **How can a standardized protocol for real-time data exchange between anti-phishing organizations be developed and validated to ensure rapid response to phishing threats?**
   - **Specific:** The question targets the development and validation of a standardized real-time data exchange protocol.
   - **Relevant:** Fills the research gap on the lack of effective real-time data sharing mechanisms that could enhance the speed of phishing detection and response.
   - **Feasible:** This could be approached through the design of protocol frameworks, followed by pilot testing with partnerships between key cybersecurity entities.
3. **What factors contribute to the longevity of phishing attacks within the detection-to-mitigation lifecycle, and how can these factors be mitigated to shorten the lifecycle?**
   - **Specific:** This question seeks to identify factors that contribute to the duration of phishing attacks from detection to mitigation.
   - **Relevant:** Addresses conflicting evidence about the impact of detection delays and the effectiveness of current mitigation efforts during the "golden hours."
   - **Feasible:** Research could be conducted by collecting and analyzing timestamped data on phishing attacks from cybersecurity databases, and testing different response strategies.

Creating a Title for Paper

논문 내용을 대략적으로 알려주고 알맞은 제목을 뽑기

Prompt

You are tasked with creating a title for a research paper. To ensure the title accurately and compellingly represents the content of the paper, use the following guidelines:

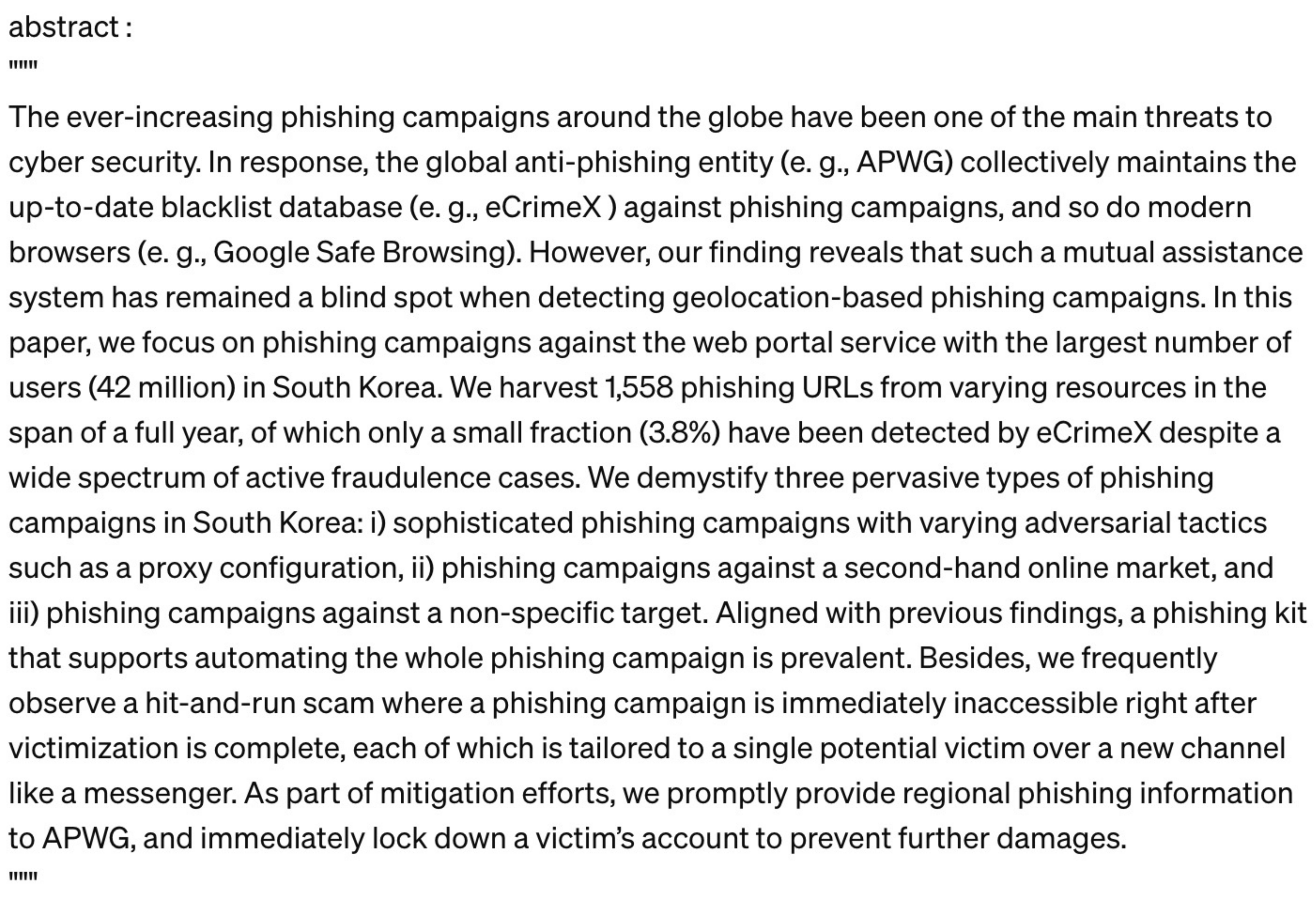
1. **Content Review**: Briefly summarize the main focus and significant findings of the research paper. Consider what the core message or contribution of the paper is.
2. **Title Characteristics**:
  - **Conciseness**: Aim for a title that is brief yet descriptive. Typically, a good title is around 10 to 20 words long.
  - **Informativeness**: Ensure the title clearly reflects the main topic and scope of the research. Include key terms that someone might use to search for your paper.
  - **Engagement**: Consider incorporating an element that can draw the reader's interest, such as a unique finding or a novel methodological approach.
3. **Generate the Title**: Combine the insights from your content review with the characteristics of a good title to formulate several title options. Select the one that best captures the essence of your research in a compelling manner.

Example Titles:
- "Exploring Neural Pathways in Decision Making: A Quantitative Analysis"
- "The Impact of Climate Change on Coastal Biodiversity: A Case Study from the Florida Keys"

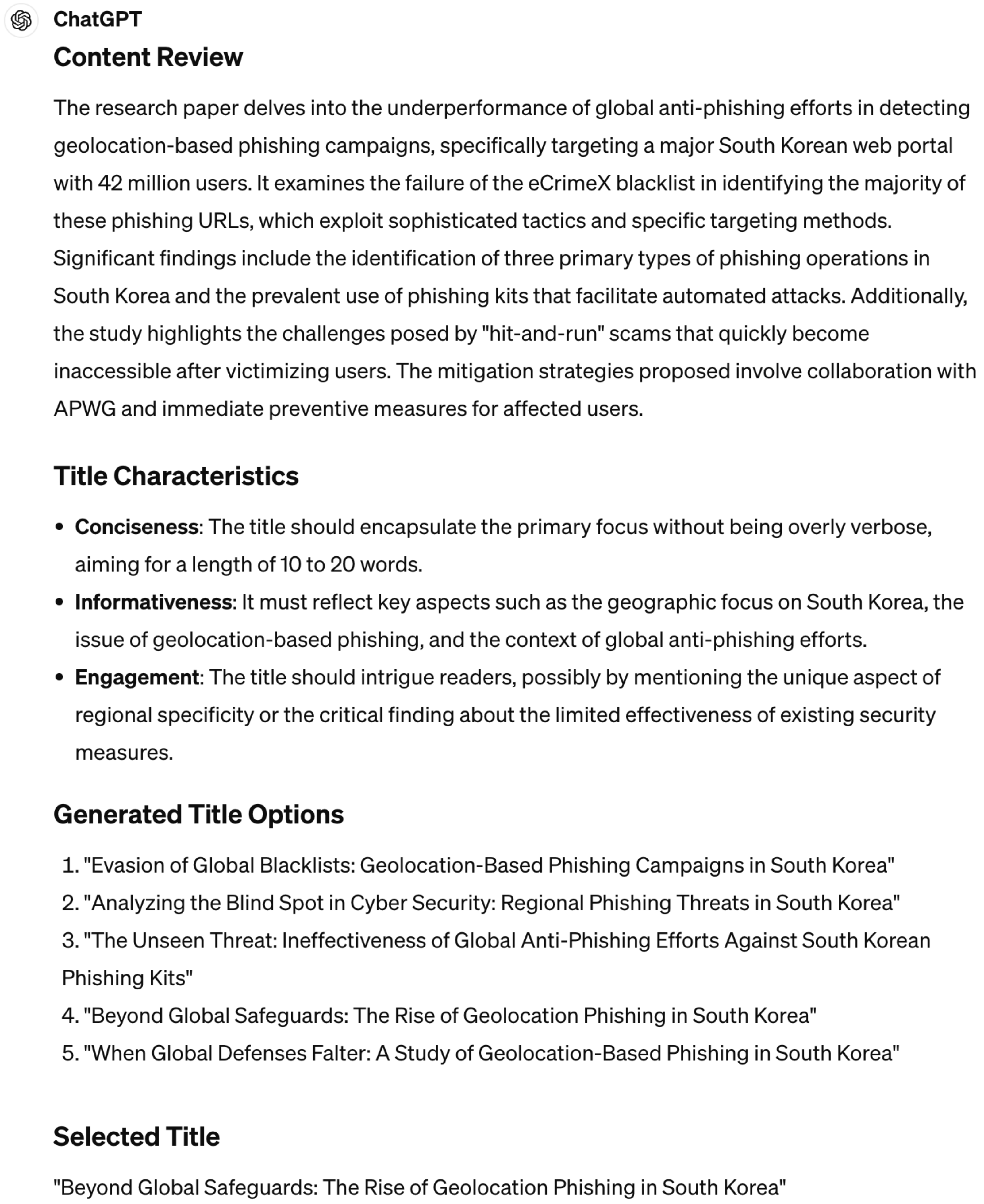
By following these steps, you can create a title that not only captures the essence of your research but also engages and informs potential readers.

Creating a Title for Paper

논문 내용을 대략적으로 알려주고 알맞은 제목을 뽑기



abstract :
"""
The ever-increasing phishing campaigns around the globe have been one of the main threats to cyber security. In response, the global anti-phishing entity (e. g., APWG) collectively maintains the up-to-date blacklist database (e. g., eCrimeX) against phishing campaigns, and so do modern browsers (e. g., Google Safe Browsing). However, our finding reveals that such a mutual assistance system has remained a blind spot when detecting geolocation-based phishing campaigns. In this paper, we focus on phishing campaigns against the web portal service with the largest number of users (42 million) in South Korea. We harvest 1,558 phishing URLs from varying resources in the span of a full year, of which only a small fraction (3.8%) have been detected by eCrimeX despite a wide spectrum of active fraudulence cases. We demystify three pervasive types of phishing campaigns in South Korea: i) sophisticated phishing campaigns with varying adversarial tactics such as a proxy configuration, ii) phishing campaigns against a second-hand online market, and iii) phishing campaigns against a non-specific target. Aligned with previous findings, a phishing kit that supports automating the whole phishing campaign is prevalent. Besides, we frequently observe a hit-and-run scam where a phishing campaign is immediately inaccessible right after victimization is complete, each of which is tailored to a single potential victim over a new channel like a messenger. As part of mitigation efforts, we promptly provide regional phishing information to APWG, and immediately lock down a victim's account to prevent further damages.
"""



ChatGPT

Content Review

The research paper delves into the underperformance of global anti-phishing efforts in detecting geolocation-based phishing campaigns, specifically targeting a major South Korean web portal with 42 million users. It examines the failure of the eCrimeX blacklist in identifying the majority of these phishing URLs, which exploit sophisticated tactics and specific targeting methods. Significant findings include the identification of three primary types of phishing operations in South Korea and the prevalent use of phishing kits that facilitate automated attacks. Additionally, the study highlights the challenges posed by "hit-and-run" scams that quickly become inaccessible after victimizing users. The mitigation strategies proposed involve collaboration with APWG and immediate preventive measures for affected users.

Title Characteristics

- **Conciseness**: The title should encapsulate the primary focus without being overly verbose, aiming for a length of 10 to 20 words.
- **Informativeness**: It must reflect key aspects such as the geographic focus on South Korea, the issue of geolocation-based phishing, and the context of global anti-phishing efforts.
- **Engagement**: The title should intrigue readers, possibly by mentioning the unique aspect of regional specificity or the critical finding about the limited effectiveness of existing security measures.

Generated Title Options

1. "Evasion of Global Blacklists: Geolocation-Based Phishing Campaigns in South Korea"
2. "Analyzing the Blind Spot in Cyber Security: Regional Phishing Threats in South Korea"
3. "The Unseen Threat: Ineffectiveness of Global Anti-Phishing Efforts Against South Korean Phishing Kits"
4. "Beyond Global Safeguards: The Rise of Geolocation Phishing in South Korea"
5. "When Global Defenses Falter: A Study of Geolocation-Based Phishing in South Korea"

Selected Title

"Beyond Global Safeguards: The Rise of Geolocation Phishing in South Korea"

Creating an concise abstract

논문의 대략적인 내용을 알려주고 abstract 뽑기

Prompt

You are tasked with creating an engaging and concise abstract for your research paper. To write an effective abstract that captures the essence of your work and interests your readers, follow these steps:

1. **Content Identification**:
  - **Objective**: Clearly state the main goal of your research. What problem are you addressing?
  - **Methods**: Summarize the methodologies you used in your research. How did you address the problem?
  - **Results**: Highlight the key findings of your research. What did you discover?
  - **Conclusions**: Conclude with the implications of your findings. What do your results mean for your field?

2. **Writing the Abstract**:
  - **Engagement**: Write in a way that is accessible and interesting to both experts and non-specialist readers. Use active voice and highlight the relevance and novelty of your findings.
  - **Conciseness**: Keep the abstract between 150 to 250 words, ensuring it briefly covers all critical aspects of your work without delving into excessive detail.

3. **Review and Refine**:
  - After drafting your abstract, review it to ensure it is clear and free of jargon. Check if it accurately reflects your research and entices readers to delve into your full paper.

Example Abstract:
"Investigating the Impact of Social Media on Public Health Perceptions: A Multidisciplinary Approach. This study examines how social media influences public health decision-making. Using a mixed-methods approach, we analyzed tweets and conducted surveys over 12 months. Findings suggest significant shifts in public health perceptions due to social media discussions. These insights could help inform future public health campaigns and policy-making."

Use this structure and guidelines to craft your abstract, making sure it serves as a compelling snapshot of your research paper.

Creating an concise abstract

논문의 대략적인 내용을 알려주고 abstract 뽑기

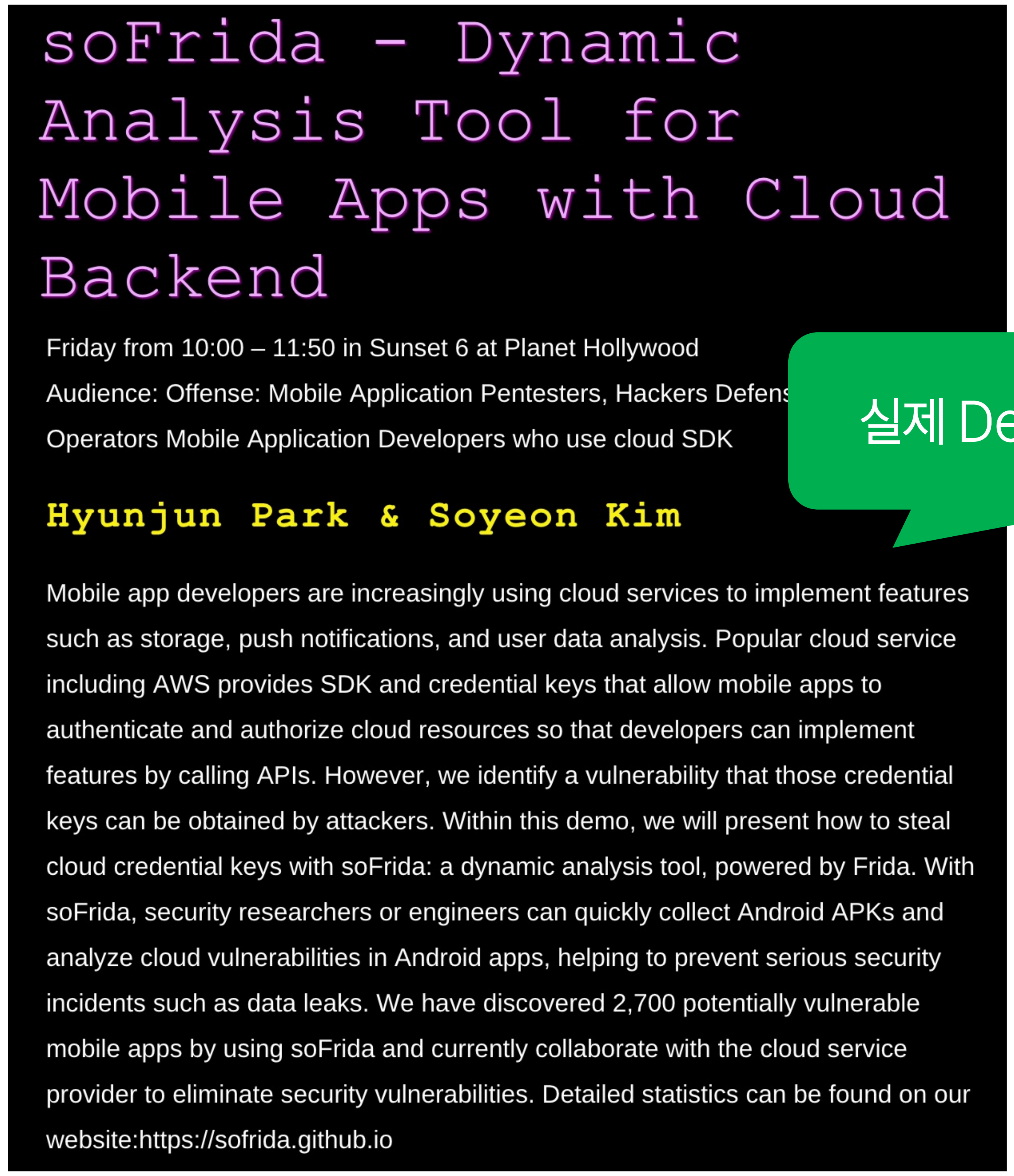
Mobile applications use a variety of cloud services, including AWS, GCP, and Azure. They are providing SDKs to facilitate the use of cloud in mobile apps. The SDKs are embedded in the mobile app and provided to the user.

The problem is that when the SDK is called, you can extract the authentication key to access the cloud service by hooking authentication-related functions. Using the frida tool, we analyzed over 1 million apps from around the world and proved that it is possible to extract authentication keys from apps that use cloud SDKs. We found vulnerabilities in 2700 apps, some of which could lead to serious privacy exposure.

GPT4 답변

Writing the Abstract

"In this study, we investigate the security vulnerabilities in mobile applications using cloud services like AWS, GCP, and Azure. By employing the Frida tool to hook into authentication functions, we analyzed over one million apps globally. Our research reveals that it is feasible to extract authentication keys, identifying vulnerabilities in 2,700 apps which could lead to serious privacy exposures. These results underscore the critical need for stronger security protocols in cloud SDKs to safeguard user data and prevent unauthorized access."



soFrida - Dynamic Analysis Tool for Mobile Apps with Cloud Backend

Friday from 10:00 – 11:50 in Sunset 6 at Planet Hollywood

Audience: Offense: Mobile Application Pentesters, Hackers Defens

Operators Mobile Application Developers who use cloud SDK

Hyunjun Park & Soyeon Kim

Mobile app developers are increasingly using cloud services to implement features such as storage, push notifications, and user data analysis. Popular cloud service including AWS provides SDK and credential keys that allow mobile apps to authenticate and authorize cloud resources so that developers can implement features by calling APIs. However, we identify a vulnerability that those credential keys can be obtained by attackers. Within this demo, we will present how to steal cloud credential keys with soFrida: a dynamic analysis tool, powered by Frida. With soFrida, security researchers or engineers can quickly collect Android APKs and analyze cloud vulnerabilities in Android apps, helping to prevent serious security incidents such as data leaks. We have discovered 2,700 potentially vulnerable mobile apps by using soFrida and currently collaborate with the cloud service provider to eliminate security vulnerabilities. Detailed statistics can be found on our website:https://sofrida.github.io

실제 Defcon 당시 abstract

Designing a research methodology

- 논문의 abstract 또는 대략적인 연구 방법을 제시하고 methodology 디자인하기

Prompt

You are tasked with designing a research methodology for your study. To ensure that your methodology is robust and suitable for addressing your research question effectively, follow these steps:

1. **Define the Research Question**:
  - Clearly state the research question or objective of your study. What are you aiming to discover or prove?

2. **Methodology Components**:
  - **Study Design**: Choose an appropriate design (e.g., experimental, observational, cross-sectional, longitudinal) based on the research question.
  - **Population and Sampling**: Describe the population for your study and the sampling technique (e.g., random, stratified, convenience) you will use to select participants.
  - **Data Collection Methods**: Outline the methods for data collection (e.g., surveys, interviews, experiments, secondary data analysis).
  - **Data Analysis**: Specify the analytical techniques (e.g., statistical analysis, thematic analysis) you will use to interpret the data.
  - **Ethical Considerations**: Address any ethical issues related to your research, including how you will ensure the confidentiality and welfare of participants.

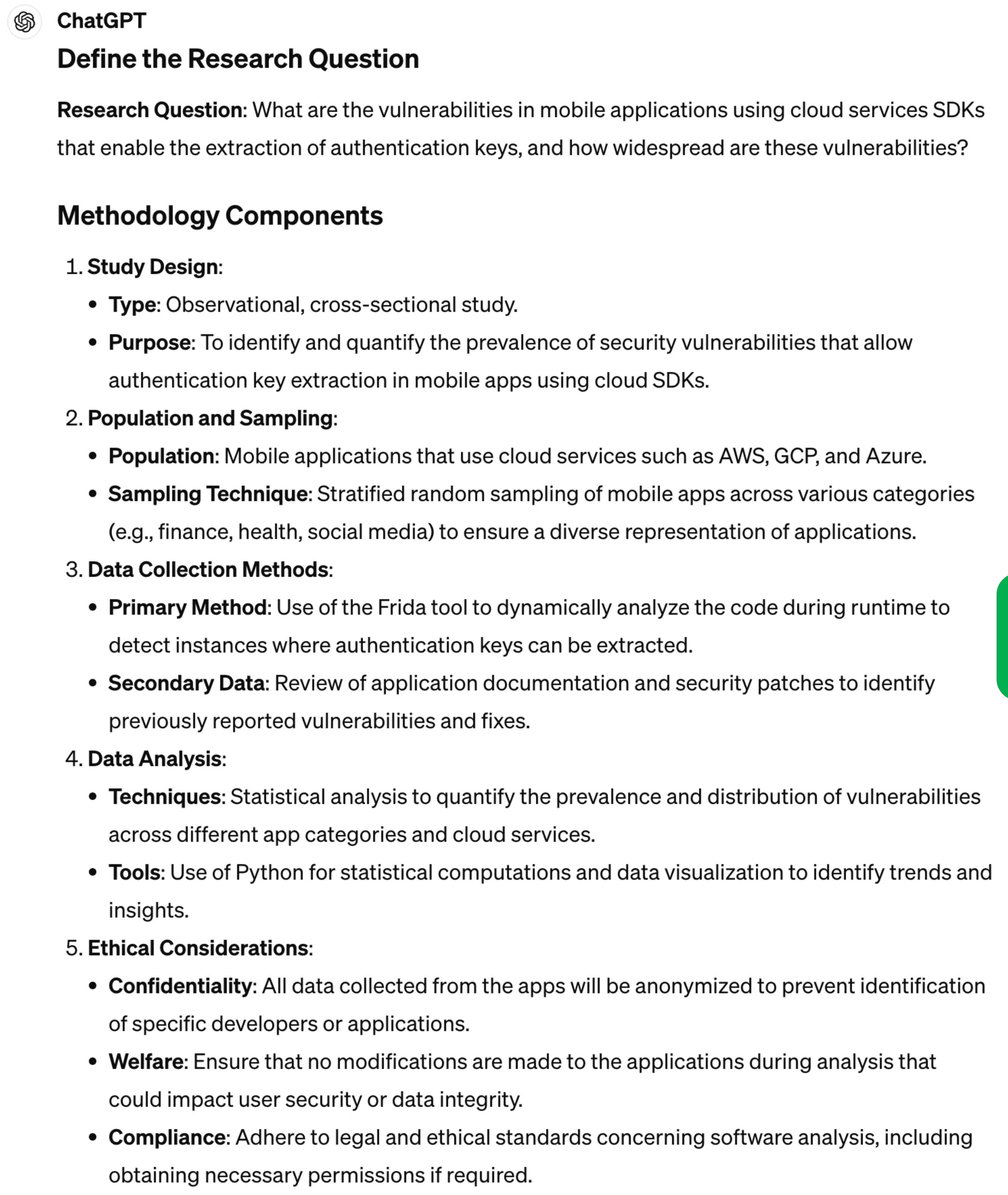
3. **Justification**:
  - Justify why each component of your methodology is the most appropriate for addressing your research question effectively.

Example Methodology:
"For our study on the impact of educational interventions on student performance, we will use a longitudinal experimental design. We will randomly select 500 students from five high schools, using stratified sampling to ensure representation across different socioeconomic backgrounds. Data will be collected through pre- and post-intervention tests and bi-monthly progress assessments. Statistical methods will be employed to analyze changes in student performance over time. All study protocols have been reviewed to ensure they adhere to ethical standards."

Use this structured approach to design a comprehensive methodology for your study, ensuring that each component is tailored to your specific research question and objectives.

Designing a research methodology

논문의 abstract 또는 대략적인 연구 방법을 제시하고 methodology 디자인하기



ChatGPT

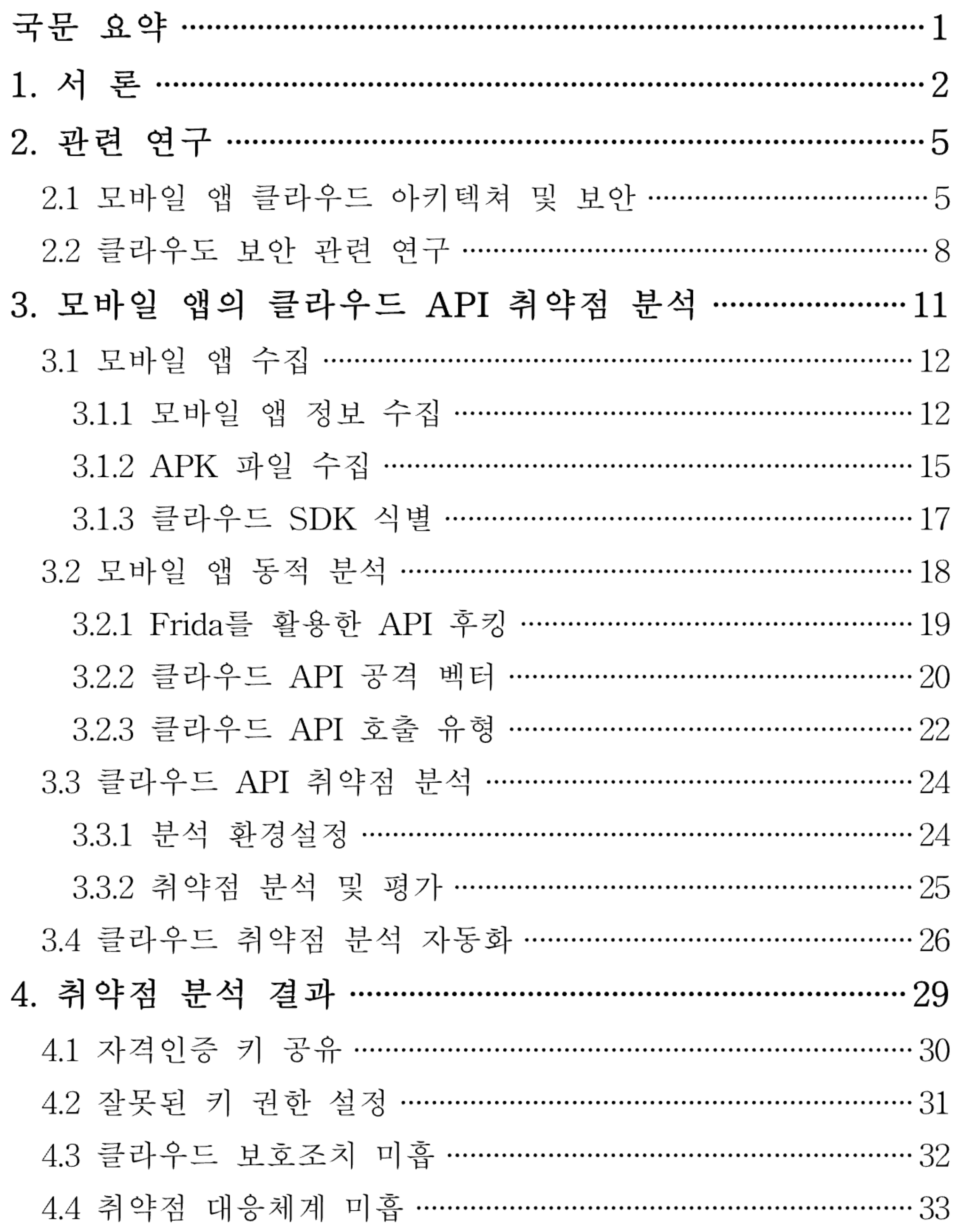
Define the Research Question

Research Question: What are the vulnerabilities in mobile applications using cloud services SDKs that enable the extraction of authentication keys, and how widespread are these vulnerabilities?

Methodology Components

1. **Study Design**:
   - **Type**: Observational, cross-sectional study.
   - **Purpose**: To identify and quantify the prevalence of security vulnerabilities that allow authentication key extraction in mobile apps using cloud SDKs.
2. **Population and Sampling**:
   - **Population**: Mobile applications that use cloud services such as AWS, GCP, and Azure.
   - **Sampling Technique**: Stratified random sampling of mobile apps across various categories (e.g., finance, health, social media) to ensure a diverse representation of applications.
3. **Data Collection Methods**:
   - **Primary Method**: Use of the Frida tool to dynamically analyze the code during runtime to detect instances where authentication keys can be extracted.
   - **Secondary Data**: Review of application documentation and security patches to identify previously reported vulnerabilities and fixes.
4. **Data Analysis**:
   - **Techniques**: Statistical analysis to quantify the prevalence and distribution of vulnerabilities across different app categories and cloud services.
   - **Tools**: Use of Python for statistical computations and data visualization to identify trends and insights.
5. **Ethical Considerations**:
   - **Confidentiality**: All data collected from the apps will be anonymized to prevent identification of specific developers or applications.
   - **Welfare**: Ensure that no modifications are made to the applications during analysis that could impact user security or data integrity.
   - **Compliance**: Adhere to legal and ethical standards concerning software analysis, including obtaining necessary permissions if required.

GPT4 답변



국문 요약 ………… 1
1. 서 론 ………… 2
2. 관련 연구 ………… 5
  2.1 모바일 앱 클라우드 아키텍처 및 보안 ………… 5
  2.2 클라우도 보안 관련 연구 ………… 8
3. 모바일 앱의 클라우드 API 취약점 분석 ………… 11
  3.1 모바일 앱 수집 ………… 12
    3.1.1 모바일 앱 정보 수집 ………… 12
    3.1.2 APK 파일 수집 ………… 15
    3.1.3 클라우드 SDK 식별 ………… 17
  3.2 모바일 앱 동적 분석 ………… 18
    3.2.1 Frida를 활용한 API 후킹 ………… 19
    3.2.2 클라우드 API 공격 벡터 ………… 20
    3.2.3 클라우드 API 호출 유형 ………… 22
  3.3 클라우드 API 취약점 분석 ………… 24
    3.3.1 분석 환경설정 ………… 24
    3.3.2 취약점 분석 및 평가 ………… 25
  3.4 클라우드 취약점 분석 자동화 ………… 26
4. 취약점 분석 결과 ………… 29
  4.1 자격인증 키 공유 ………… 30
  4.2 잘못된 키 권한 설정 ………… 31
  4.3 클라우드 보호조치 미흡 ………… 32
  4.4 취약점 대응체계 미흡 ………… 33

실제 졸업 논문 목차

Data Analysis with LLM

데이터셋으로 부터 의미있는 내용을 추출하고 필요한 경우 그래프를 생성하기

Prompt

You have been provided with a dataset containing a list of phishing sites collected over the past year. To effectively analyze this data and illustrate your findings, follow these steps:

1. **Data Familiarization**:
  - Examine the dataset to understand its structure. Identify key data points such as IP addresses, URLs, domain registration dates, geographical locations, and timestamps.

2. **Specific Analysis Tasks**:
  - **IP Address Analysis**: Determine which IP addresses are most frequently associated with phishing sites. Assess if these IPs share common characteristics, such as geographical origins or frequency of occurrence across different phishing sites.
  - **Temporal Patterns**: Identify any patterns in the timing of phishing site activities, such as particular times of year or specific events that trigger an increase in phishing activities.

3. **Visualization of Findings**:
  - Based on your analysis, choose a type of chart that best represents your data. For example, use a bar chart to show the frequency of IP addresses, or a heat map to depict geographical distribution.
  - Utilize data visualization tools (e.g., Tableau, Microsoft Excel, or Python with matplotlib) to create your chart.

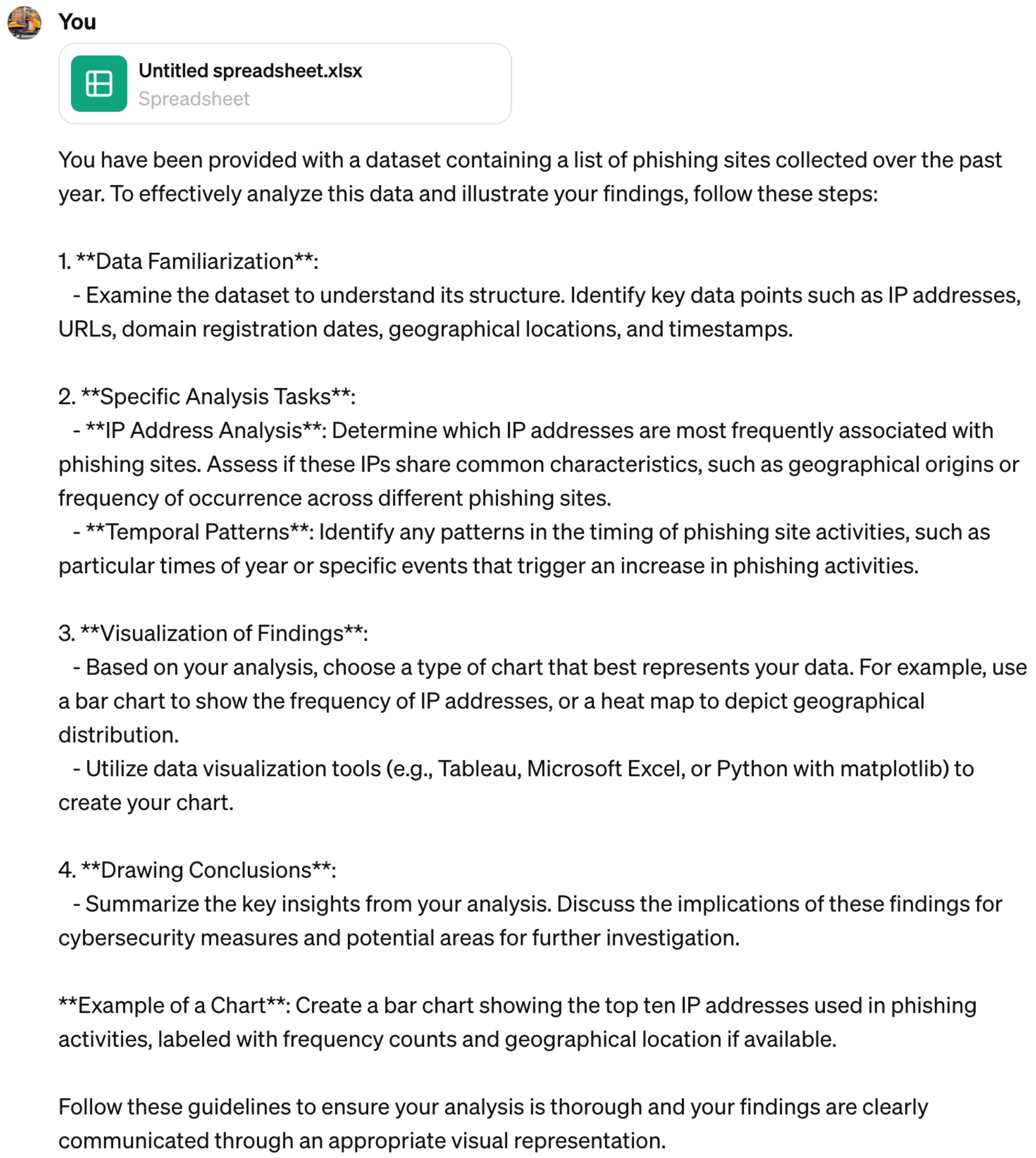
4. **Drawing Conclusions**:
  - Summarize the key insights from your analysis. Discuss the implications of these findings for cybersecurity measures and potential areas for further investigation.

Example of a Chart: Create a bar chart showing the top ten IP addresses used in phishing activities, labeled with frequency counts and geographical location if available.

Follow these guidelines to ensure your analysis is thorough and your findings are clearly communicated through an appropriate visual representation.

Data Analysis with LLM

데이터셋으로 부터 의미있는 내용을 추출하고 필요한 경우 그래프를 생성하기



You have been provided with a dataset containing a list of phishing sites collected over the past year. To effectively analyze this data and illustrate your findings, follow these steps:

1. **Data Familiarization**:
   - Examine the dataset to understand its structure. Identify key data points such as IP addresses, URLs, domain registration dates, geographical locations, and timestamps.

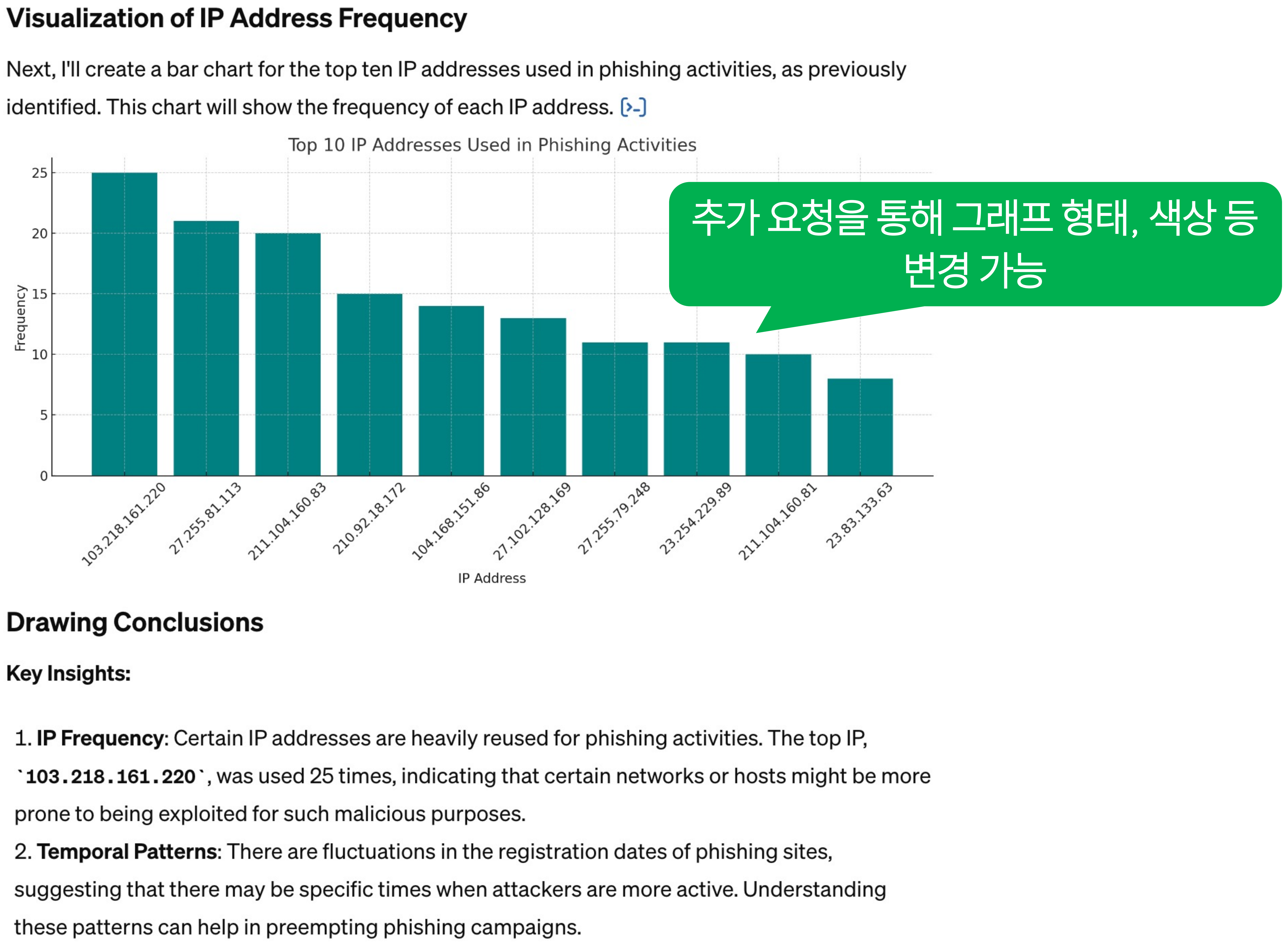
2. **Specific Analysis Tasks**:
   - **IP Address Analysis**: Determine which IP addresses are most frequently associated with phishing sites. Assess if these IPs share common characteristics, such as geographical origins or frequency of occurrence across different phishing sites.
   - **Temporal Patterns**: Identify any patterns in the timing of phishing site activities, such as particular times of year or specific events that trigger an increase in phishing activities.

3. **Visualization of Findings**:
   - Based on your analysis, choose a type of chart that best represents your data. For example, use a bar chart to show the frequency of IP addresses, or a heat map to depict geographical distribution.
   - Utilize data visualization tools (e.g., Tableau, Microsoft Excel, or Python with matplotlib) to create your chart.

4. **Drawing Conclusions**:
   - Summarize the key insights from your analysis. Discuss the implications of these findings for cybersecurity measures and potential areas for further investigation.

Example of a Chart: Create a bar chart showing the top ten IP addresses used in phishing activities, labeled with frequency counts and geographical location if available.

Follow these guidelines to ensure your analysis is thorough and your findings are clearly communicated through an appropriate visual representation.



Visualization of IP Address Frequency

Next, I'll create a bar chart for the top ten IP addresses used in phishing activities, as previously identified. This chart will show the frequency of each IP address. [>-]

추가 요청을 통해 그래프 형태, 색상 등 변경 가능

Drawing Conclusions

Key Insights:

1. **IP Frequency**: Certain IP addresses are heavily reused for phishing activities. The top IP, `103.218.161.220`, was used 25 times, indicating that certain networks or hosts might be more prone to being exploited for such malicious purposes.
2. **Temporal Patterns**: There are fluctuations in the registration dates of phishing sites, suggesting that there may be specific times when attackers are more active. Understanding these patterns can help in preempting phishing campaigns.

Describing figure legend

- 주어진 figure에 대한 legend 작성하기

Prompt

Attached are multiple figures (e.g., Fig. 1, Fig. 2) intended for inclusion in my work-in-progress scientific paper. Please review the provided results notes and use them to write detailed legends for each figure. Each legend should:

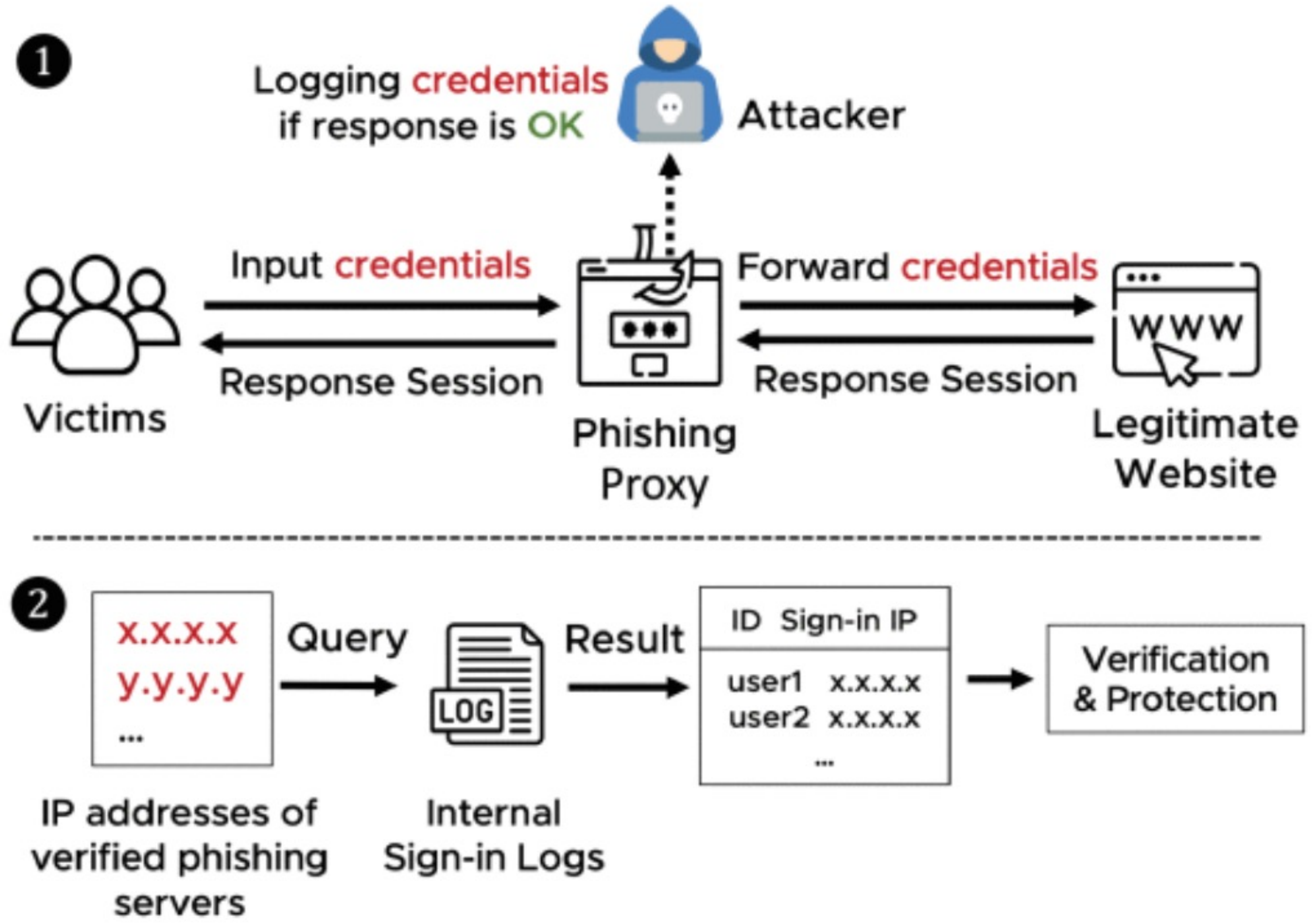
1. **Briefly Describe the Figure**: Summarize what the figure represents, including key variables and the nature of the data presented.
2. **Incorporate Results Notes**: Highlight critical findings from the results notes related to the figure, such as significant data points, statistical tests used, or any conclusions drawn.
3. **Meet Journal Standards**: Ensure each legend adheres to the standards of scientific journals, which require clarity, conciseness, and specific details like sample size, p-values, or experimental conditions, where applicable.

Your task is to ensure that these legends effectively communicate the significance and context of each figure to a scholarly audience.

Describing figure legend

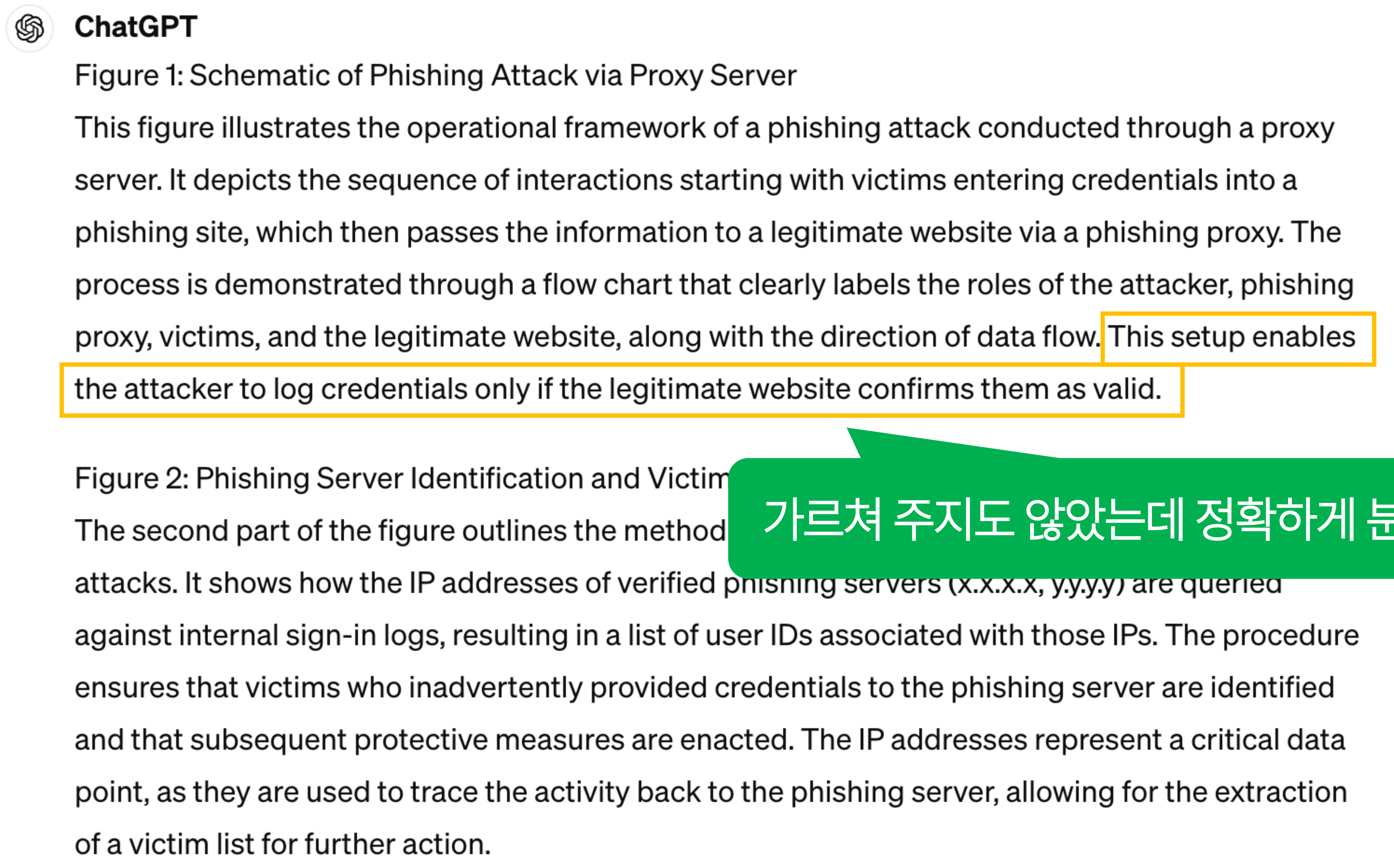
주어진 figure에 대한 legend 작성하기

You



1. the attacker establishes a proxy phishing server to lure the victim. When the victim connects to the proxy phishing server, the proxy server communicates with the legitimate server as if the victim had connected to the legitimate site.

2. Since the proxy server is relaying communication with the legitimate server, the IP of the victim is recorded as the IP of the proxy server when the victim connects to the phishing server. This allows us to extract a list of victims and take protective measures.



ChatGPT

Figure 1: Schematic of Phishing Attack via Proxy Server

This figure illustrates the operational framework of a phishing attack conducted through a proxy server. It depicts the sequence of interactions starting with victims entering credentials into a phishing site, which then passes the information to a legitimate website via a phishing proxy. The process is demonstrated through a flow chart that clearly labels the roles of the attacker, phishing proxy, victims, and the legitimate website, along with the direction of data flow. This setup enables the attacker to log credentials only if the legitimate website confirms them as valid.

Figure 2: Phishing Server Identification and Victim

The second part of the figure outlines the method

attacks. It shows how the IP addresses of verified phishing servers (x.x.x.x, y.y.y.y) are queried against internal sign-in logs, resulting in a list of user IDs associated with those IPs. The procedure ensures that victims who inadvertently provided credentials to the phishing server are identified and that subsequent protective measures are enacted. The IP addresses represent a critical data point, as they are used to trace the activity back to the phishing server, allowing for the extraction of a victim list for further action.

가르쳐 주지도 않았는데 정확하게 분석함

Converting to Latex

실제 논문을 작성하기 위한 Latex 문서로 변환하기

Prompt

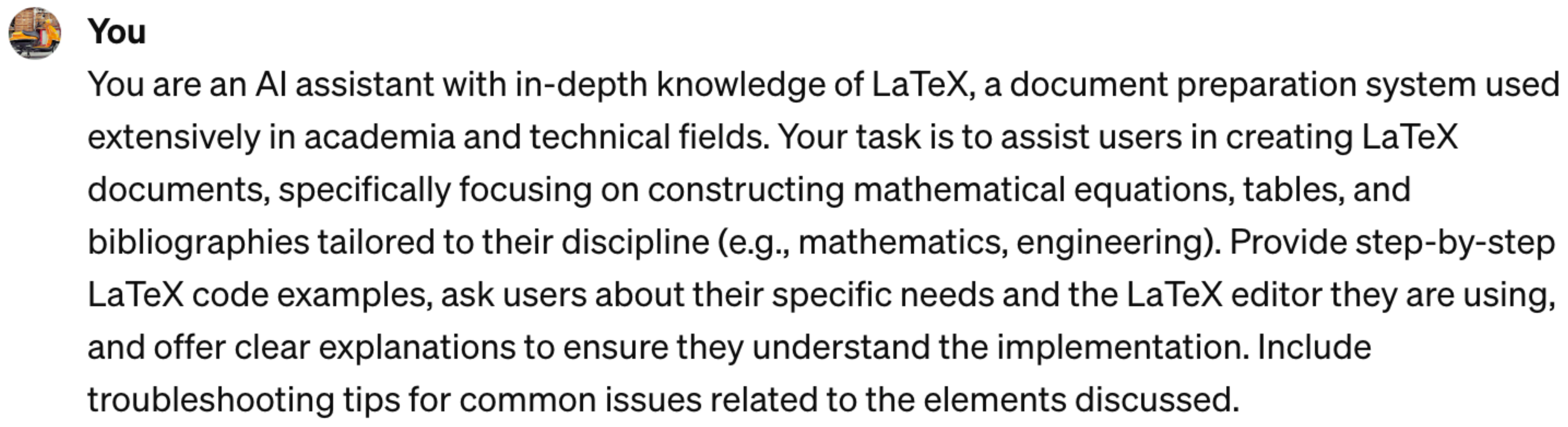
You are an AI assistant with in-depth knowledge of LaTeX, a document preparation system used extensively in academia and technical fields.

Your task is to assist users in creating LaTeX documents, specifically focusing on constructing mathematical equations, tables, and bibliographies tailored to their discipline (e.g., mathematics, engineering). Provide step-by-step LaTeX code examples, ask users about their specific needs and the LaTeX editor they are using, and offer clear explanations to ensure they understand the implementation. Include troubleshooting tips for common issues related to the elements discussed.

- Latex Environment : {Overleaf / TexShop / Tex Live}

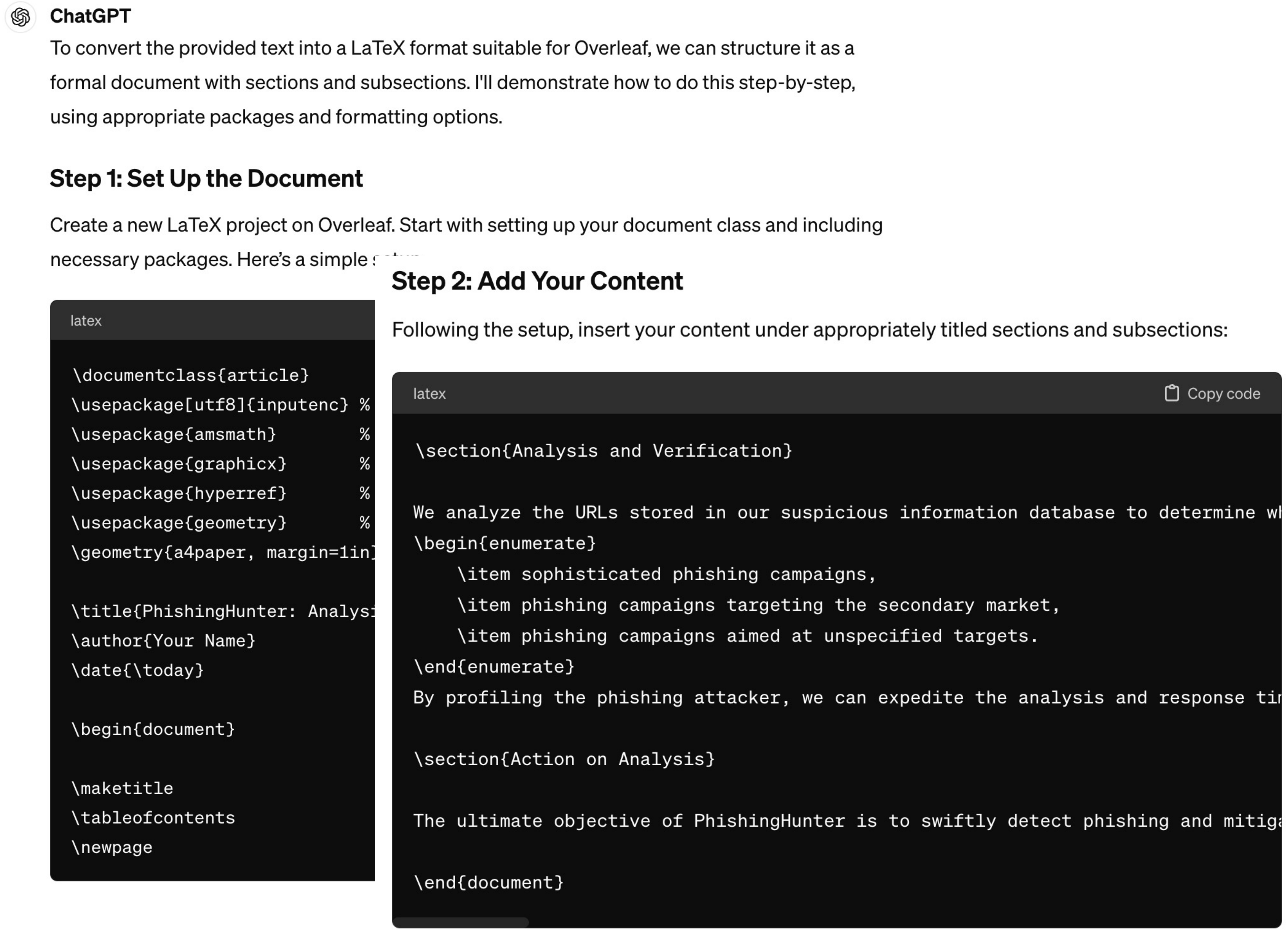
Converting to Latex

실제 논문을 작성하기 위한 Latex 문서로 변환하기



You

You are an AI assistant with in-depth knowledge of LaTeX, a document preparation system used extensively in academia and technical fields. Your task is to assist users in creating LaTeX documents, specifically focusing on constructing mathematical equations, tables, and bibliographies tailored to their discipline (e.g., mathematics, engineering). Provide step-by-step LaTeX code examples, ask users about their specific needs and the LaTeX editor they are using, and offer clear explanations to ensure they understand the implementation. Include troubleshooting tips for common issues related to the elements discussed.



ChatGPT

To convert the provided text into a LaTeX format suitable for Overleaf, we can structure it as a formal document with sections and subsections. I'll demonstrate how to do this step-by-step, using appropriate packages and formatting options.

Step 1: Set Up the Document

Create a new LaTeX project on Overleaf. Start with setting up your document class and including necessary packages. Here's a simple s

```latex
\documentclass{article}
\usepackage[utf8]{inputenc} %
\usepackage{amsmath}        %
\usepackage{graphicx}       %
\usepackage{hyperref}       %
\usepackage{geometry}       %
\geometry{a4paper, margin=1in

\title{PhishingHunter: Analysi
\author{Your Name}
\date{\today}

\begin{document}

\maketitle
\tableofcontents
\newpage
```

Step 2: Add Your Content

Following the setup, insert your content under appropriately titled sections and subsections:

```latex
\section{Analysis and Verification}

We analyze the URLs stored in our suspicious information database to determine wh
\begin{enumerate}
    \item sophisticated phishing campaigns,
    \item phishing campaigns targeting the secondary market,
    \item phishing campaigns aimed at unspecified targets.
\end{enumerate}
By profiling the phishing attacker, we can expedite the analysis and response ti

\section{Action on Analysis}

The ultimate objective of PhishingHunter is to swiftly detect phishing and mitig

\end{document}
```

Polishing

어색한 문장을 논문용으로 다시 작성하기

Prompt

* Context: Introduction Section Review
* Purpose: I am revisiting the introduction section of my academic paper and require specific feedback on a problematic sentence.
* Issue: The sentence in question disrupts the flow and clarity of the introduction, making it sound awkward.
* Task: Please provide a detailed analysis explaining why the sentence might sound awkward. Additionally, suggest specific revisions to enhance clarity and coherence.
* Sentence: [Insert awkward sentence here]

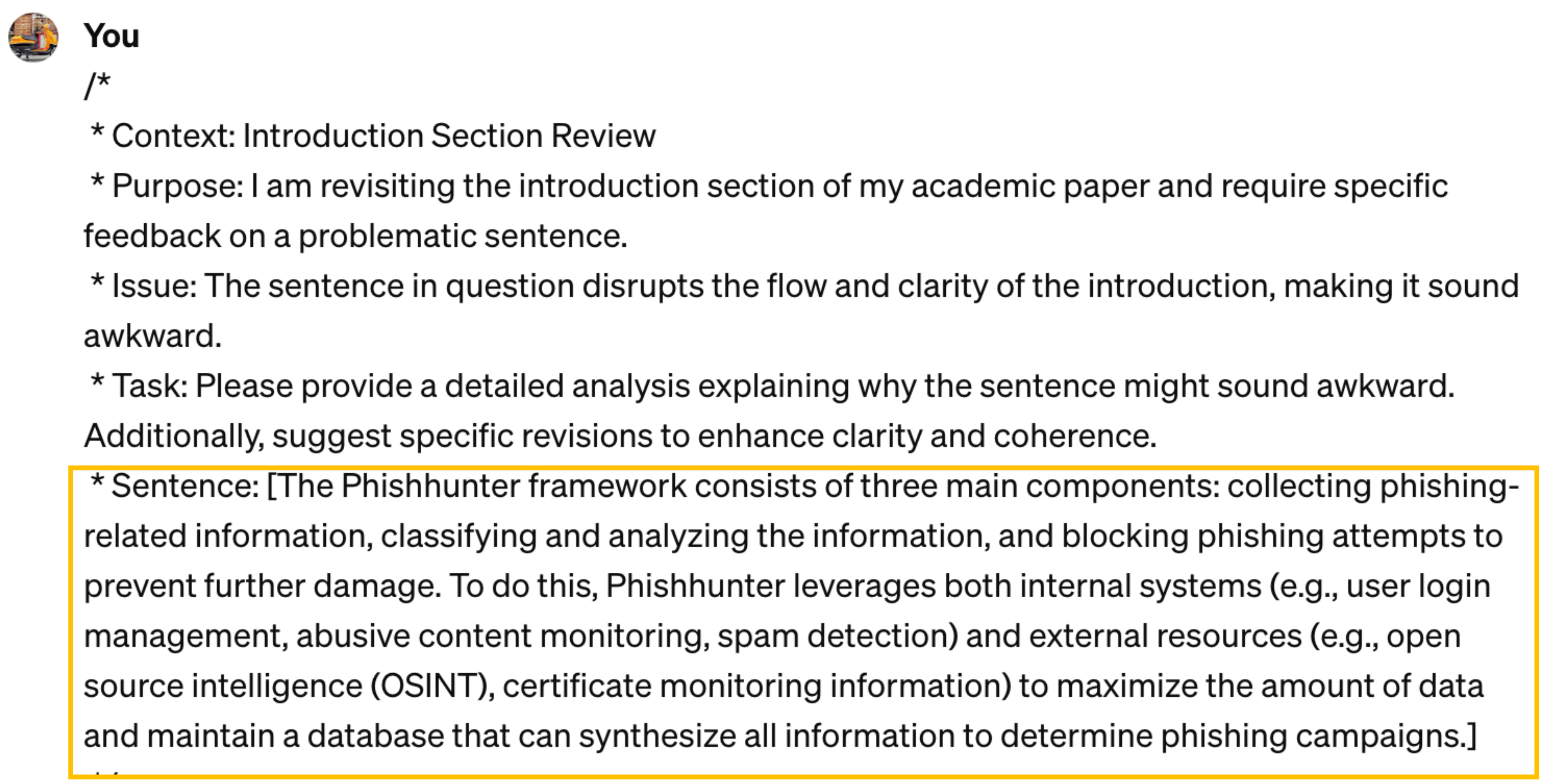
Prompt

"I am preparing a manuscript on [specific topic, e.g., 'the impact of climate change on urban planning'] for submission to a prestigious journal in [specific discipline, e.g., 'environmental science']. The key argument I try to make in the following section is [specific point, e.g., 'that current urban planning policies are insufficient to mitigate climate risks'].

Please rephrase this section to enhance clarity (ensure the argument is straightforward), improve coherence (link ideas smoothly), and increase conciseness (eliminate unnecessary words). Avoid technical jargon, such as 'anthropogenic,' and replace it with more accessible language like 'human-caused.' Ensure the tone remains professional, utilizing formal language and avoiding colloquial expressions."

Polishing

어색한 문장을 논문용으로 다시 작성하기



You

/*

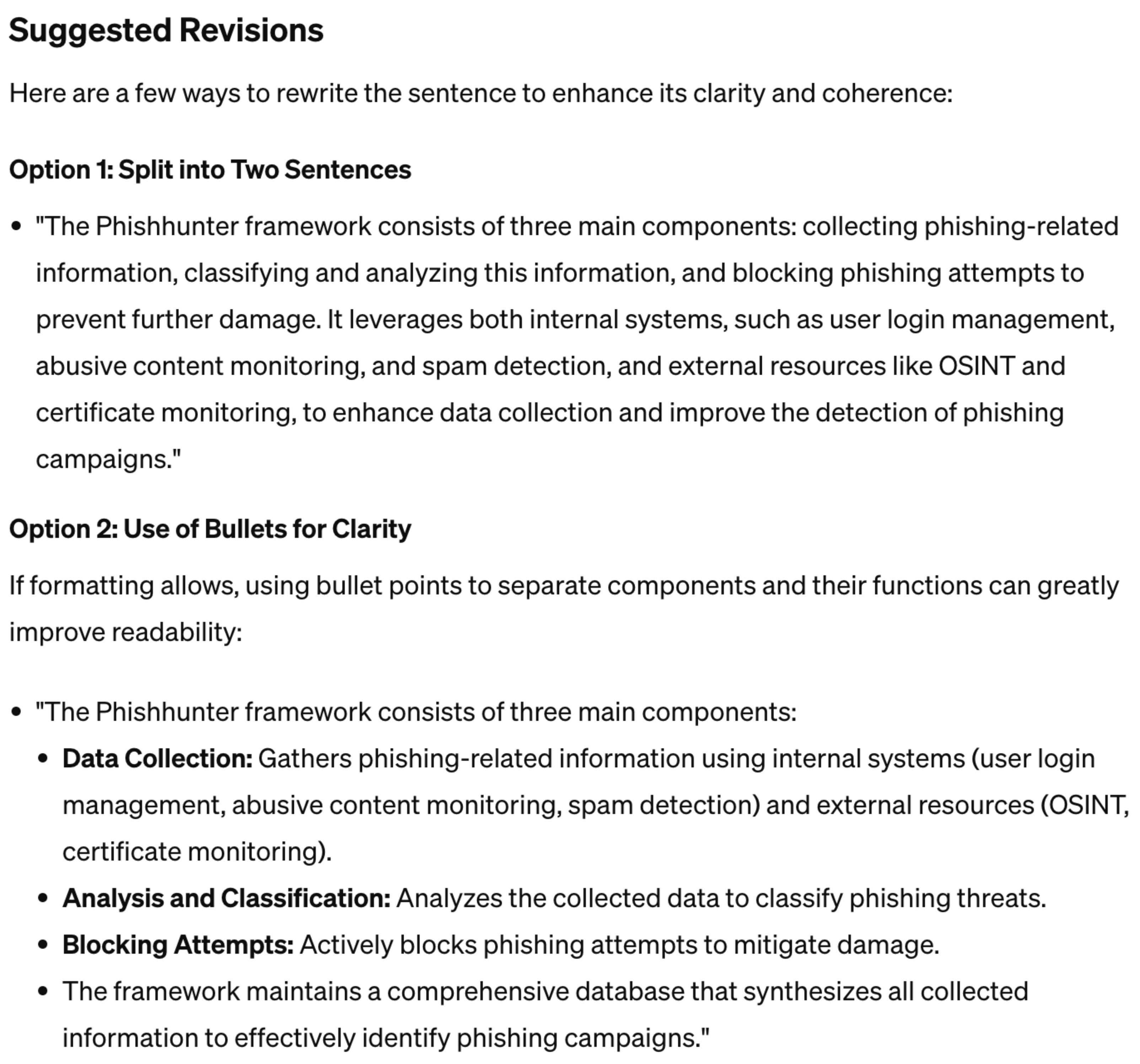
* Context: Introduction Section Review

* Purpose: I am revisiting the introduction section of my academic paper and require specific feedback on a problematic sentence.

* Issue: The sentence in question disrupts the flow and clarity of the introduction, making it sound awkward.

* Task: Please provide a detailed analysis explaining why the sentence might sound awkward. Additionally, suggest specific revisions to enhance clarity and coherence.

* Sentence: [The Phishhunter framework consists of three main components: collecting phishing-related information, classifying and analyzing the information, and blocking phishing attempts to prevent further damage. To do this, Phishhunter leverages both internal systems (e.g., user login management, abusive content monitoring, spam detection) and external resources (e.g., open source intelligence (OSINT), certificate monitoring information) to maximize the amount of data and maintain a database that can synthesize all information to determine phishing campaigns.]



Suggested Revisions

Here are a few ways to rewrite the sentence to enhance its clarity and coherence:

Option 1: Split into Two Sentences

- "The Phishhunter framework consists of three main components: collecting phishing-related information, classifying and analyzing this information, and blocking phishing attempts to prevent further damage. It leverages both internal systems, such as user login management, abusive content monitoring, and spam detection, and external resources like OSINT and certificate monitoring, to enhance data collection and improve the detection of phishing campaigns."

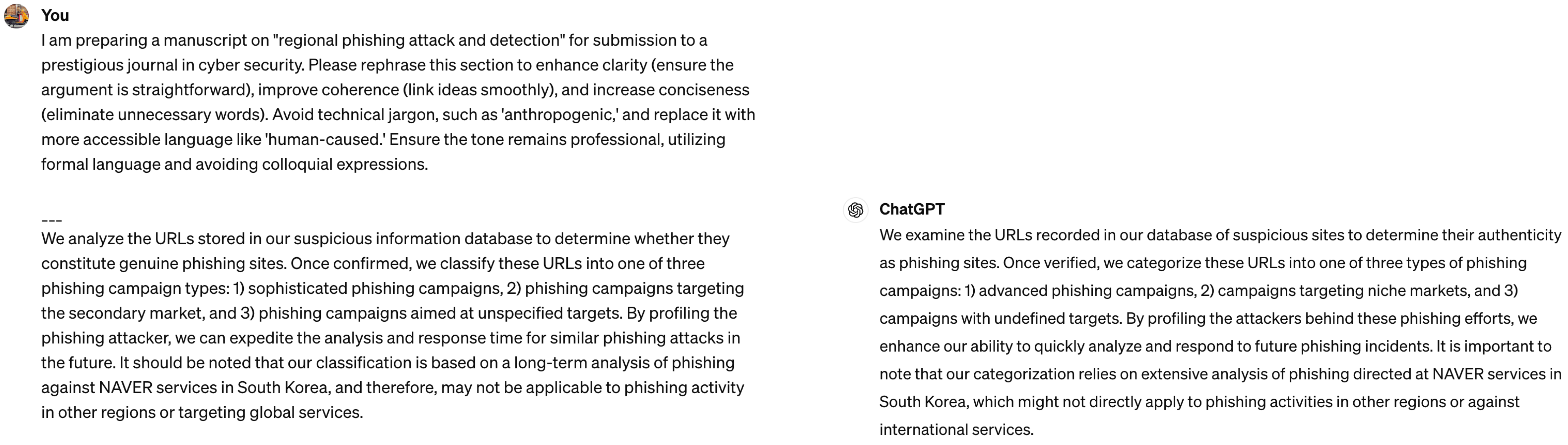
Option 2: Use of Bullets for Clarity

If formatting allows, using bullet points to separate components and their functions can greatly improve readability:

- "The Phishhunter framework consists of three main components:
  - **Data Collection:** Gathers phishing-related information using internal systems (user login management, abusive content monitoring, spam detection) and external resources (OSINT, certificate monitoring).
  - **Analysis and Classification:** Analyzes the collected data to classify phishing threats.
  - **Blocking Attempts:** Actively blocks phishing attempts to mitigate damage.
  - The framework maintains a comprehensive database that synthesizes all collected information to effectively identify phishing campaigns."

Polishing

어색한 문장을 논문용으로 다시 작성하기



You

I am preparing a manuscript on "regional phishing attack and detection" for submission to a prestigious journal in cyber security. Please rephrase this section to enhance clarity (ensure the argument is straightforward), improve coherence (link ideas smoothly), and increase conciseness (eliminate unnecessary words). Avoid technical jargon, such as 'anthropogenic,' and replace it with more accessible language like 'human-caused.' Ensure the tone remains professional, utilizing formal language and avoiding colloquial expressions.

---

We analyze the URLs stored in our suspicious information database to determine whether they constitute genuine phishing sites. Once confirmed, we classify these URLs into one of three phishing campaign types: 1) sophisticated phishing campaigns, 2) phishing campaigns targeting the secondary market, and 3) phishing campaigns aimed at unspecified targets. By profiling the phishing attacker, we can expedite the analysis and response time for similar phishing attacks in the future. It should be noted that our classification is based on a long-term analysis of phishing against NAVER services in South Korea, and therefore, may not be applicable to phishing activity in other regions or targeting global services.

ChatGPT

We examine the URLs recorded in our database of suspicious sites to determine their authenticity as phishing sites. Once verified, we categorize these URLs into one of three types of phishing campaigns: 1) advanced phishing campaigns, 2) campaigns targeting niche markets, and 3) campaigns with undefined targets. By profiling the attackers behind these phishing efforts, we enhance our ability to quickly analyze and respond to future phishing incidents. It is important to note that our categorization relies on extensive analysis of phishing directed at NAVER services in South Korea, which might not directly apply to phishing activities in other regions or against international services.

Review your paper

논문 제출전에 미리 리뷰어로 부터 받을 수 있는 질문에 대비하기

Prompt

Acting as a strict reviewer for a high-impact biomedical journal, conduct a thorough and detailed critique of the provided article. Your assessment should meticulously evaluate the article's methodology, clarity of writing, novelty, and ethical considerations. Ensure all your critiques are constructive and supported by evidence. Use the following structured format for your feedback:

Methodology
- Assess the robustness and appropriateness of the research methods used.
- Comment on the sample size, control variables, and any statistical analyses employed.
- Identify any methodological flaws or areas for improvement.

Clarity of Writing:
- Evaluate the organization and presentation of the article.
- Note any sections that are unclear or poorly written.
- Suggest specific improvements for enhancing readability and understanding.

Novelty:
- Determine the originality of the research and its contribution to the field.
- Discuss whether the findings add new insights or merely replicate previous studies.
- Suggest how the work could be modified to increase its impact and originality.

Ethical Considerations:
- Review compliance with ethical guidelines in the conduct of research.
- Comment on the adequacy of patient consent forms, if applicable.
- Highlight any potential ethical issues not addressed by the authors.

Feedback Structure:
- Major Concerns:
  - List significant issues that impact the validity, reliability, or integrity of the work.
  - Provide evidence or examples to support each concern.

- Minor Concerns:
  - Note smaller issues that could improve the paper's quality if addressed.
  - Offer specific suggestions for corrections or enhancements.

End your review by summarizing the overall strengths and weaknesses of the article, ensuring that your critique is balanced and fair.

Review your paper

논문 제출전에 미리 리뷰어로 부터 받을 수 있는 질문에 대비하기

Prompt

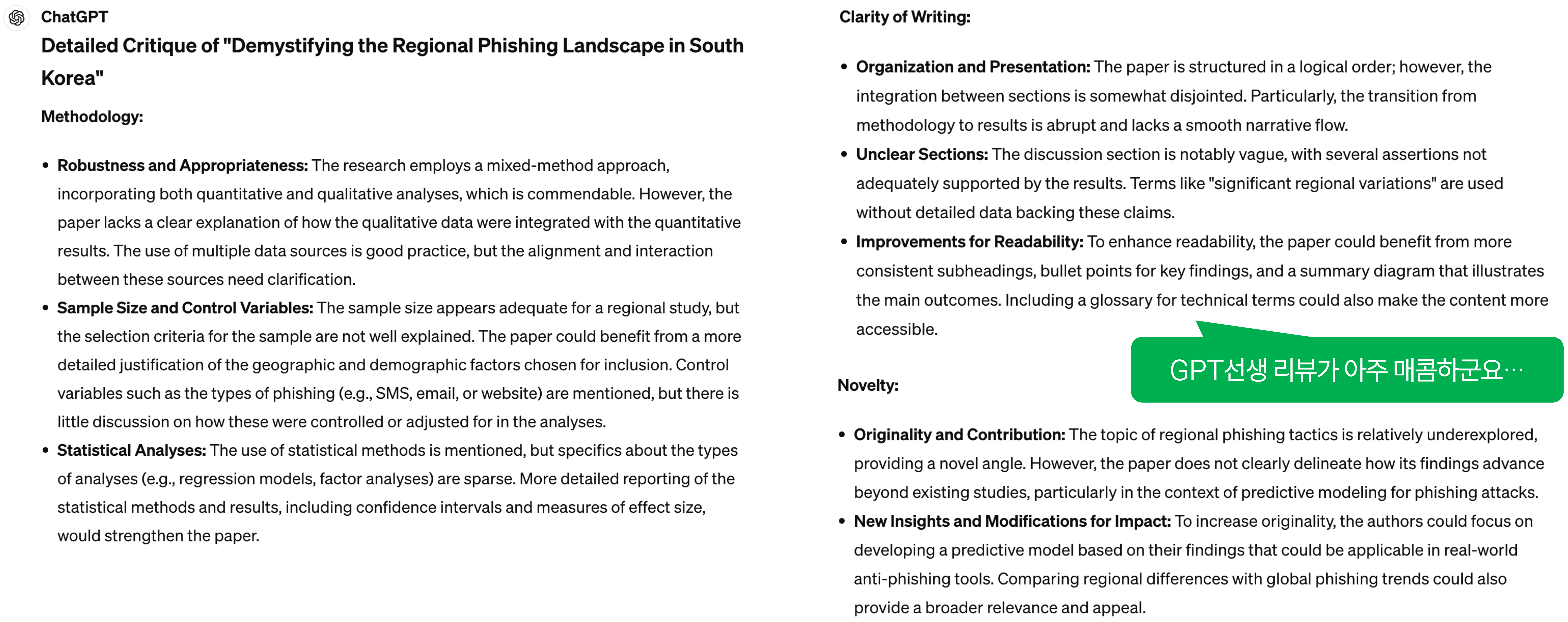
Assume you are a panel of experts with over 20 years of academic experience in [specific field], such as environmental science, theoretical physics, or cultural anthropology. Based on my summary of a paper focused on [specific topic, e.g., the effects of climate change on urban infrastructure], provide a detailed review of this paper. Structure your response as follows：

1) Core Content： Summarize the main arguments, methodology, and findings of the paper.
2) Limitations： Identify and discuss the key limitations of the study, citing specific examples or areas of concern.
3) Significance of Limitations： Explain the importance of each identified limitation in order of their impact on the field or the study's findings.

Please use bullet points for each section to maintain a concise and professional tone.

Review your paper

논문 제출전에 미리 리뷰어로 부터 받을 수 있는 질문에 대비하기



ChatGPT

Detailed Critique of "Demystifying the Regional Phishing Landscape in South Korea"

Methodology:

- **Robustness and Appropriateness:** The research employs a mixed-method approach, incorporating both quantitative and qualitative analyses, which is commendable. However, the paper lacks a clear explanation of how the qualitative data were integrated with the quantitative results. The use of multiple data sources is good practice, but the alignment and interaction between these sources need clarification.
- **Sample Size and Control Variables:** The sample size appears adequate for a regional study, but the selection criteria for the sample are not well explained. The paper could benefit from a more detailed justification of the geographic and demographic factors chosen for inclusion. Control variables such as the types of phishing (e.g., SMS, email, or website) are mentioned, but there is little discussion on how these were controlled or adjusted for in the analyses.
- **Statistical Analyses:** The use of statistical methods is mentioned, but specifics about the types of analyses (e.g., regression models, factor analyses) are sparse. More detailed reporting of the statistical methods and results, including confidence intervals and measures of effect size, would strengthen the paper.

Clarity of Writing:

- **Organization and Presentation:** The paper is structured in a logical order; however, the integration between sections is somewhat disjointed. Particularly, the transition from methodology to results is abrupt and lacks a smooth narrative flow.
- **Unclear Sections:** The discussion section is notably vague, with several assertions not adequately supported by the results. Terms like "significant regional variations" are used without detailed data backing these claims.
- **Improvements for Readability:** To enhance readability, the paper could benefit from more consistent subheadings, bullet points for key findings, and a summary diagram that illustrates the main outcomes. Including a glossary for technical terms could also make the content more accessible.

Novelty:

- **Originality and Contribution:** The topic of regional phishing tactics is relatively underexplored, providing a novel angle. However, the paper does not clearly delineate how its findings advance beyond existing studies, particularly in the context of predictive modeling for phishing attacks.
- **New Insights and Modifications for Impact:** To increase originality, the authors could focus on developing a predictive model based on their findings that could be applicable in real-world anti-phishing tools. Comparing regional differences with global phishing trends could also provide a broader relevance and appeal.

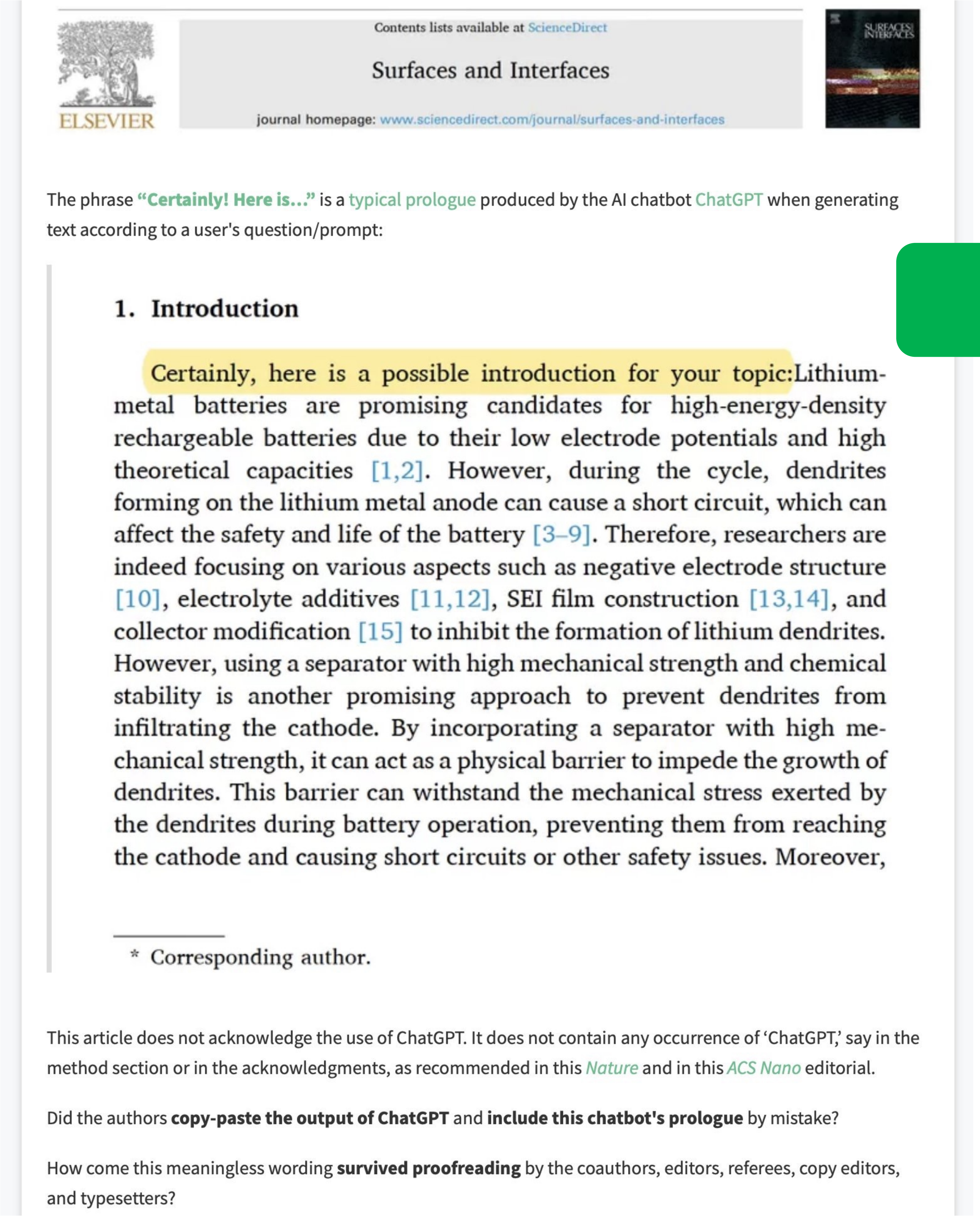
GPT선생 리뷰가 아주 매콤하군요…

Ethics & Conclusion

Regulations for using LLM

- 인공지능이 생성한 결과물의 진실성을 보장할 수 없고 출처를 확실하게 추적하고 신뢰할 수 없기 때문에, 과학적 결과물에 대한 최종 책임은 항상 사람이 져야 한다.
- AI 도구에 민감 정보를 업로드할 때는 개인정보보호, 기밀정보보호, 지식재산권과 관련된 이슈들에 특별히 주의해야 함
- LLM에 모든 것을 의존해서는 안되며, 논문 작성시 어려운 부분을 도와주는 용도로만 활용할 것을 추천

Regulations for using LLM



Contents lists available at ScienceDirect

Surfaces and Interfaces

journal homepage: www.sciencedirect.com/journal/surfaces-and-interfaces

The phrase **"Certainly! Here is…"** is a typical prologue produced by the AI chatbot ChatGPT when generating text according to a user's question/prompt:

> **1. Introduction**
>
> Certainly, here is a possible introduction for your topic:Lithium-metal batteries are promising candidates for high-energy-density rechargeable batteries due to their low electrode potentials and high theoretical capacities [1,2]. However, during the cycle, dendrites forming on the lithium metal anode can cause a short circuit, which can affect the safety and life of the battery [3–9]. Therefore, researchers are indeed focusing on various aspects such as negative electrode structure [10], electrolyte additives [11,12], SEI film construction [13,14], and collector modification [15] to inhibit the formation of lithium dendrites. However, using a separator with high mechanical strength and chemical stability is another promising approach to prevent dendrites from infiltrating the cathode. By incorporating a separator with high mechanical strength, it can act as a physical barrier to impede the growth of dendrites. This barrier can withstand the mechanical stress exerted by the dendrites during battery operation, preventing them from reaching the cathode and causing short circuits or other safety issues. Moreover,
>
> ---
>
> * Corresponding author.

This article does not acknowledge the use of ChatGPT. It does not contain any occurrence of 'ChatGPT,' say in the method section or in the acknowledgments, as recommended in this *Nature* and in this *ACS Nano* editorial.

Did the authors **copy-paste the output of ChatGPT** and **include this chatbot's prologue** by mistake?

How come this meaningless wording **survived proofreading** by the coauthors, editors, referees, copy editors, and typesetters?

복/붙의 결말은… Reject

Conclusion

- LLM을 통해 연구자들이 가장 고통 받는 영역중 하나였던 [언어 장벽]을 극복할 수 있음
- 논문 작성의 전체 과정에서 활용할 수 있으며, 명확한 프롬프트 엔지니어링을 통해 더 좋은 결과를 얻을 수 있음
  - [자료 수집 및 요약,분석] / [초록 및 본문 작성] / [데이터 분석] / [문법 첨삭] / [피어 리뷰 준비]
- 프롬프트 엔지니어링에 정답은 없음. 계속해서 연구하고 발전시켜서 나만의 훌륭한 비서를 만들것.

References

- https://youtu.be/CkCL8dV_mPk?si=YGJ1fcCRBIcQt6-G(인지적 프롬프트 공유회)
- Gemini for Google Workspace Prompt Guide (https://inthecloud.withgoogle.com/gemini-for-google-workspace-prompt-guide/dl-cd.html)
- https://steady-study.super.site/self-evloving-chatgpt-prompt
- Wang, Zhenhailong, et al. "Unleashing the emergent cognitive synergy in large language models: A task-solving agent through multi-persona self-collaboration." arXiv preprint arXiv:2307.05300 (2023).
- https://www.nature.com/articles/d41586-024-01042-3
- 이미지 : unsplash.com

Thank You