BÁO CÁO

BÀI TẬP 3: VIẾT PROMPT HIỆU QUẢ CHO CÁC TÁC VỤ HỌC TẬP

Họ và tên: Nguyễn Phú Cường

MSV: 25050504

Lớp: QH-2025E KTPT3

Môn học: Nhập môn Công nghệ số và Ứng dụng Trí tuệ nhân tạo

1. Mở đầu

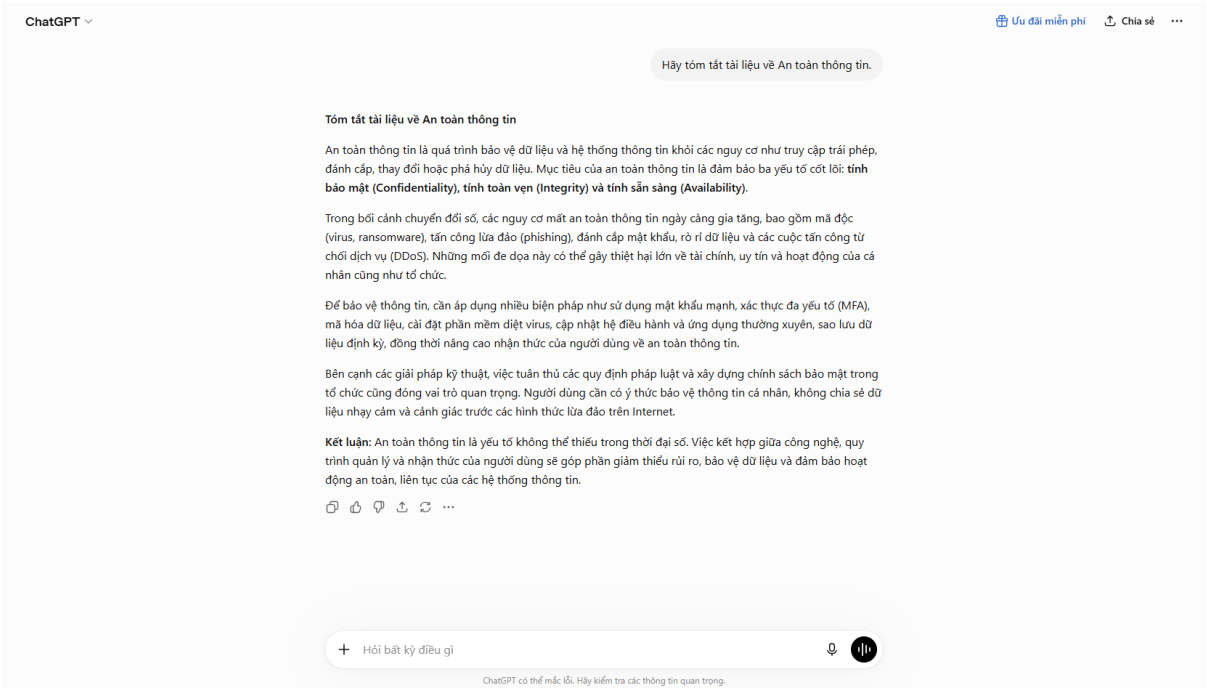
Trong bối cảnh AI được ứng dụng rộng rãi trong học tập, việc viết prompt hiệu quả giúp khai thác tối đa khả năng của mô hình ngôn ngữ lớn. Chất lượng prompt quyết định mức độ đầy đủ, chính xác và có cấu trúc của kết quả. Báo cáo này lựa chọn ba tác vụ học tập phổ biến: tóm tắt tài liệu, giải thích khái niệm và tạo câu hỏi ôn tập. Mỗi tác vụ được xây dựng với ba mức prompt (cơ bản, cải tiến, nâng cao), thử nghiệm bằng ChatGPT, sau đó so sánh và rút ra các nguyên tắc viết prompt hiệu quả.

2. Tóm tắt tài liệu học thuật

Mục tiêu: tóm tắt tài liệu học thuật về chủ đề An toàn thông tin.

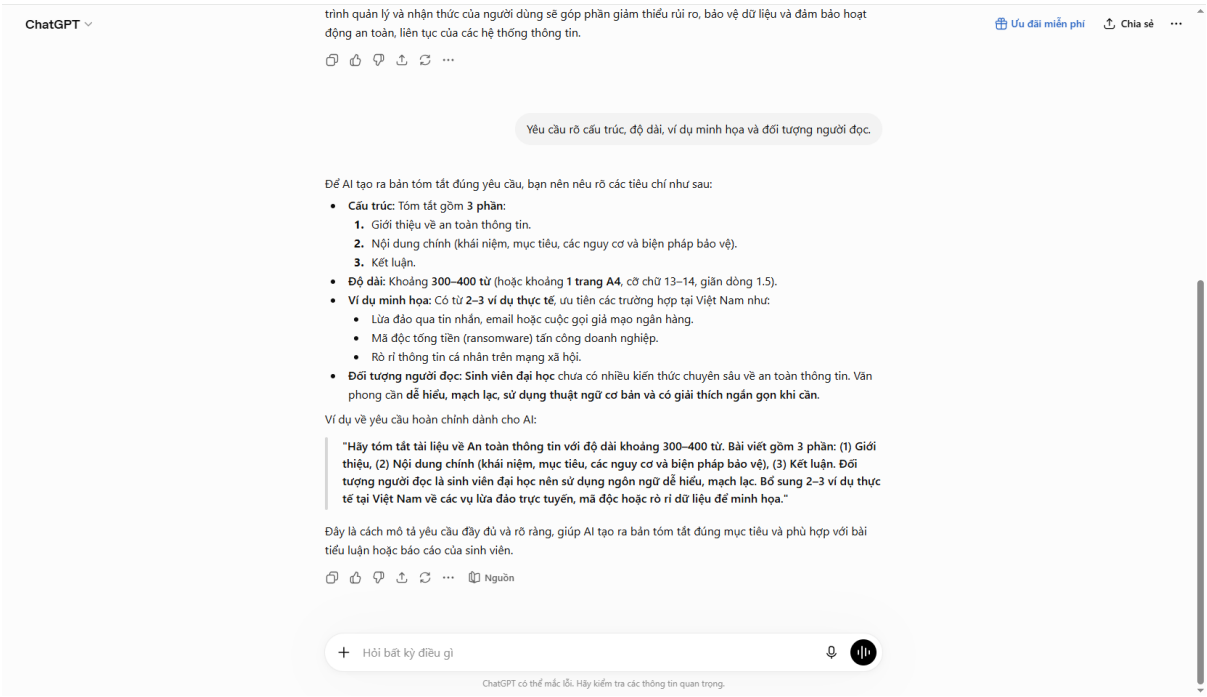
Prompt cơ bản

Hãy tóm tắt tài liệu về An toàn thông tin.



Prompt cải tiến

Yêu cầu rõ cấu trúc, độ dài, ví dụ minh họa và đối tượng người đọc.



Prompt nâng cao

Bạn là sinh viên đại học. Thực hiện nhiệm vụ theo từng mục rõ ràng, có ví dụ, giải thích, trình bày dạng bullet, độ dài phù hợp.

ChatGPT

Nguồn

Ưu đãi miễn phí

Chia sẻ

Bạn là sinh viên đại học. Thực hiện nhiệm vụ theo từng mục rõ ràng, có ví dụ, giải thích, trình bày dạng bullet, độ dài phù hợp.

Sửa

Tóm tắt tài liệu về An toàn thông tin

1. Giới thiệu

An toàn thông tin là việc bảo vệ dữ liệu, hệ thống và các tài nguyên thông tin khỏi những hành vi truy cập trái phép, đánh cắp, sửa đổi hoặc phá hủy. Trong thời đại chuyển đổi số, hầu hết các hoạt động học tập, làm việc và giao dịch đều diễn ra trên môi trường Internet, vì vậy việc đảm bảo an toàn thông tin ngày càng trở nên quan trọng đối với cá nhân, doanh nghiệp và cơ quan nhà nước.

---

2. Nội dung chính

2.1. Khái niệm an toàn thông tin

- An toàn thông tin là tập hợp các biện pháp kỹ thuật và quản lý nhằm bảo vệ thông tin trước các nguy cơ trên không gian mạng.
- Mục tiêu là đảm bảo thông tin luôn được lưu trữ, truyền tải và sử dụng một cách an toàn.

Ba nguyên tắc cốt lõi (CIA):

- **Tính bảo mật (Confidentiality):** Chỉ người được cấp quyền mới có thể truy cập thông tin.
- **Tính toàn vẹn (Integrity):** Dữ liệu không bị thay đổi hoặc chỉnh sửa trái phép.
- **Tính sẵn sàng (Availability):** Hệ thống và dữ liệu luôn sẵn sàng khi người dùng cần.

Ví dụ:

- Hệ thống quản lý điểm của trường đại học chỉ cho phép giảng viên và sinh viên có tài khoản hợp lệ truy cập. Điều này giúp bảo vệ thông tin cá nhân và kết quả học tập.

2.2. Các nguy cơ mất an toàn thông tin

Một số nguy cơ phổ biến gồm:

- **Virus và mã độc (Malware):**
  - Xâm nhập vào máy tính để đánh cắp hoặc phá hủy dữ liệu.
  - Có thể làm chậm hệ thống hoặc khóa toàn bộ dữ liệu.

Hỏi bất kỳ điều gì

ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.

ChatGPT

Sửa

Ưu đãi miễn phí

Chia sẻ

- **Virus và mã độc (Malware):**
  - Xâm nhập vào máy tính để đánh cắp hoặc phá hủy dữ liệu.
  - Có thể làm chậm hệ thống hoặc khóa toàn bộ dữ liệu.
- **Lừa đảo trực tuyến (Phishing):**
  - Kẻ gian giả mạo ngân hàng, trường học hoặc cơ quan nhà nước để lấy mật khẩu, mã OTP.
  - Thường xuất hiện qua email, tin nhắn hoặc mạng xã hội.
- **Rò rỉ dữ liệu cá nhân:**
  - Thông tin như số điện thoại, CCCD hoặc tài khoản ngân hàng bị phát tán trên Internet.
  - Có thể dẫn đến lừa đảo hoặc chiếm đoạt tài sản.
- **Tấn công từ chối dịch vụ (DDoS):**
  - Làm quá tải hệ thống khiến website hoặc dịch vụ trực tuyến không thể hoạt động bình thường.

Ví dụ thực tế:

- Nhiều người tại Việt Nam nhận được cuộc gọi giả danh công an hoặc nhân viên ngân hàng yêu cầu chuyển tiền để "xác minh tài khoản", dẫn đến mất tiền.
- Một số doanh nghiệp bị mã độc tống tiền (Ransomware), khiến dữ liệu bị mã hóa và phải tạm dừng hoạt động.

2.3. Biện pháp bảo vệ an toàn thông tin

Để giảm thiểu rủi ro, cần thực hiện các biện pháp sau:

- Sử dụng mật khẩu mạnh, có độ dài từ 10–12 kí tự và kết hợp chữ hoa, chữ thường, số và kí tự đặc biệt.
- Bật xác thực hai yếu tố (2FA/MFA) cho các tài khoản quan trọng.
- Cập nhật hệ điều hành và phần mềm thường xuyên để vá lỗ hổng bảo mật.
- Cài đặt phần mềm diệt virus có uy tín.
- Sao lưu dữ liệu định kỳ trên ổ cứng hoặc dịch vụ lưu trữ đám mây.
- Không nhấp vào liên kết hoặc tải tệp từ nguồn không đáng tin cậy.
- Hạn chế chia sẻ thông tin cá nhân trên mạng xã hội.
- Kiểm tra kỹ địa chỉ website trước khi đăng nhập hoặc thực hiện giao dịch.

Ví dụ:

- Khi đăng nhập Gmail hoặc tài khoản ngân hàng, người dùng nên bật xác thực hai yếu tố để tăng cường bảo mật ngay cả khi mật khẩu bị lộ.

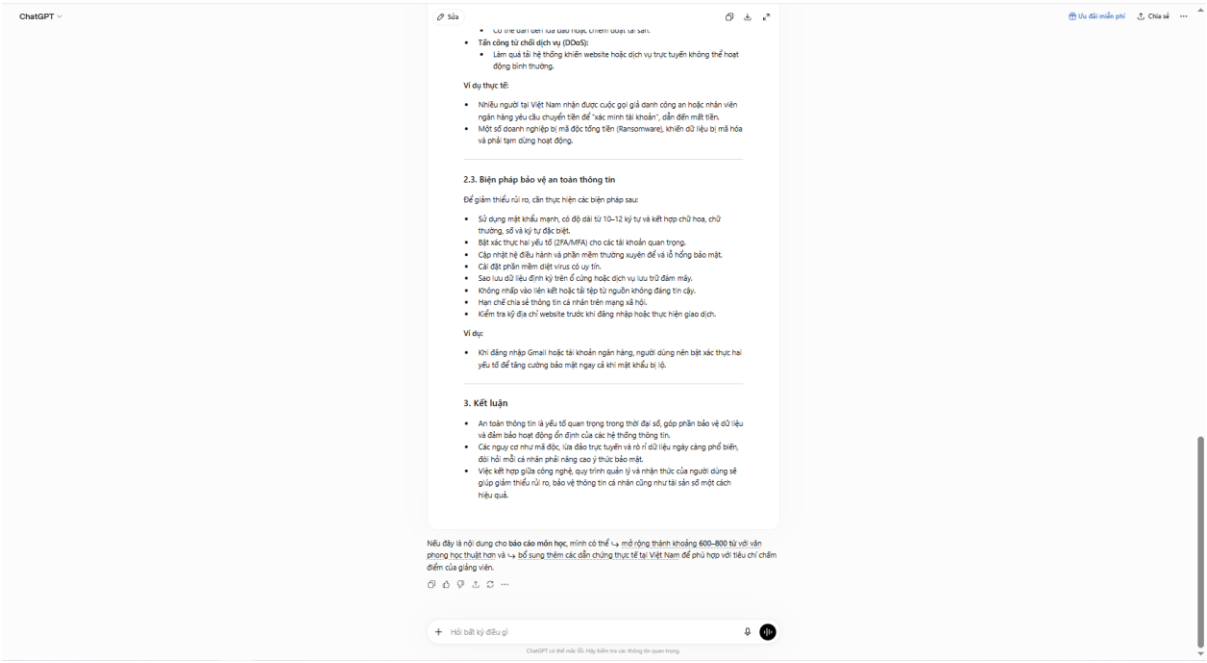
---

3. Kết luận

- An toàn thông tin là yếu tố quan trọng trong thời đại số, góp phần bảo vệ dữ liệu và đảm bảo hoạt động ổn định của các hệ thống thông tin.
- Các nguy cơ như mã độc, lừa đảo trực tuyến và rò rỉ dữ liệu ngày càng phổ biến, đòi hỏi mỗi cá nhân phải nâng cao ý thức bảo mật.
- Việc kết hợp giữa công nghệ, quy trình, quản lý và nhận thức của người dùng sẽ giúp giảm thiểu rủi ro, bảo vệ thông tin cá nhân cũng như tài sản số một cách

Hỏi bất kỳ điều gì

ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.



So sánh kết quả

Tiêu chí	Cơ bản	Cải tiến	Nâng cao
Độ đầy đủ	Thấp	Khá	Rất tốt
Cấu trúc	Ít	Rõ	Rất rõ
Ví dụ	Không	Có	Có nhiều
Khả năng áp dụng	TB	Tốt	Rất tốt

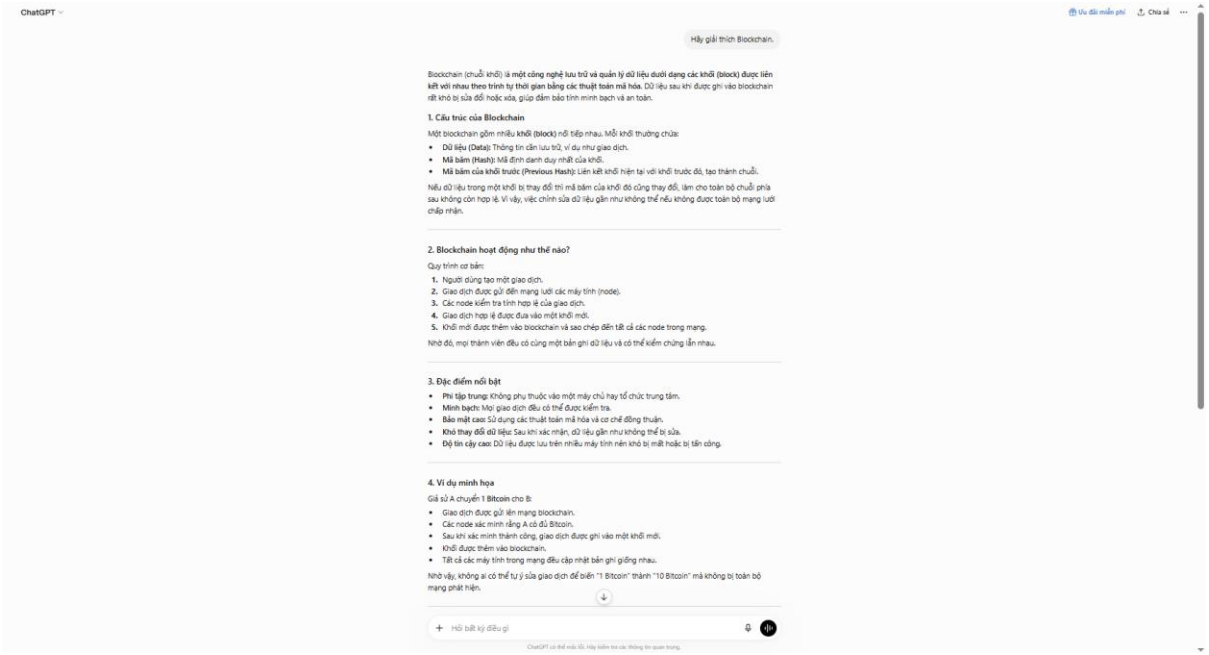
Nhận xét: Prompt nâng cao cho kết quả tốt nhất nhờ cung cấp đầy đủ bối cảnh, vai trò, định dạng và yêu cầu cụ thể.

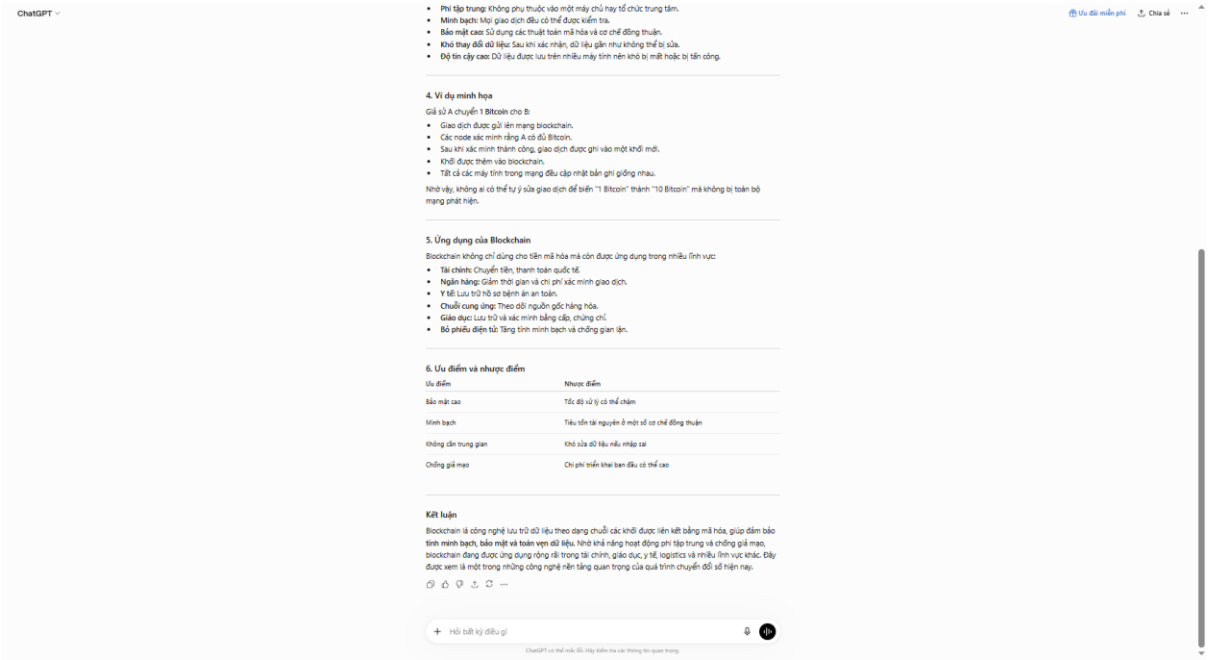
3. Giải thích khái niệm phức tạp

Mục tiêu: giải thích khái niệm phức tạp về chủ đề Blockchain.

Prompt cơ bản

Hãy giải thích Blockchain.





Prompt cải tiến

Yêu cầu rõ cấu trúc, độ dài, ví dụ minh họa và đối tượng người đọc.

ChatGPT

Ưu đãi miễn phí | Chia sẻ

Hãy giải thích Blockchain. Yêu cầu rõ cấu trúc, độ dài, ví dụ minh họa và đối tượng người đọc.

Giải thích Blockchain

1. Đối tượng người đọc

- **Sinh viên đại học**, đặc biệt các ngành Công nghệ thông tin, Hệ thống thông tin, Thương mại điện tử, Kinh tế số.
- Người mới bắt đầu tìm hiểu về Blockchain và tiền mã hóa.
- Độc giả không yêu cầu có kiến thức chuyên sâu về lập trình.

---

2. Độ dài

- **Khoảng 800 từ**.
- Trình bày đầy đủ khái niệm, cấu trúc, nguyên lý hoạt động, đặc điểm, ưu điểm, hạn chế và ứng dụng.
- Phù hợp làm nội dung cho bài tiểu luận hoặc báo cáo học phần.

---

3. Cấu trúc nội dung

3.1. Khái niệm Blockchain

Blockchain (chuỗi khối) là **công nghệ lưu trữ và quản lý dữ liệu theo dạng chuỗi các khối (Block), trong đó mỗi khối được liên kết với khối trước bằng một mã băm (Hash)**. Dữ liệu sau khi được ghi vào Blockchain gần như không thể sửa đổi hoặc xóa bỏ nếu không có sự đồng thuận của toàn bộ mạng lưới. Điều này giúp đảm bảo tính toàn vẹn, minh bạch và an toàn của dữ liệu.

Khác với cơ sở dữ liệu truyền thống chỉ được quản lý bởi một tổ chức hoặc máy chủ trung tâm, Blockchain hoạt động theo mô hình **phi tập trung (Decentralized)**. Mỗi máy tính tham gia mạng (gọi là **Node**) đều lưu giữ một bản sao của toàn bộ Blockchain. Nhờ vậy, nếu một máy tính gặp sự cố hoặc bị tấn công, dữ liệu vẫn được bảo toàn trên các máy còn lại.

3.2. Cấu trúc của Blockchain

Mỗi Blockchain gồm nhiều khối dữ liệu liên kết với nhau theo thứ tự thời gian. Một khối thường bao gồm ba thành phần chính:

- **Data (Dữ liệu):** Chứa thông tin cần lưu trữ, chẳng hạn như giao dịch tài chính, hợp đồng hoặc hồ sơ.
- **Hash (Mã băm):** Là chuỗi ký tự được tạo bằng thuật toán mã hóa, đóng vai trò như "dấu vân tay" của khối. Mỗi khối có một mã băm duy nhất.
- **Previous Hash (Mã băm của khối trước):** Liên kết khối hiện tại với khối trước đó, tạo thành một chuỗi liên tục.

Nếu dữ liệu trong một khối bị thay đổi, mã băm của [illegible] đó cũng thay đổi, làm mất tính liên kết với các khối tiếp theo. Vì vậy, việc chỉnh sửa dữ liệu trên Blockchain gần như không khả thi.

Hỏi bất kỳ điều gì

ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.

ChatGPT

Ưu đãi miễn phí | Chia sẻ

thành phần chính:

- **Data (Dữ liệu):** Chứa thông tin cần lưu trữ, chẳng hạn như giao dịch tài chính, hợp đồng hoặc hồ sơ.
- **Hash (Mã băm):** Là chuỗi ký tự được tạo bằng thuật toán mã hóa, đóng vai trò như "dấu vân tay" của khối. Mỗi khối có một mã băm duy nhất.
- **Previous Hash (Mã băm của khối trước):** Liên kết khối hiện tại với khối trước đó, tạo thành một chuỗi liên tục.

Nếu dữ liệu trong một khối bị thay đổi, mã băm của khối đó cũng thay đổi, làm mất tính liên kết với các khối tiếp theo. Vì vậy, việc chỉnh sửa dữ liệu trên Blockchain gần như không khả thi.

3.3. Nguyên lý hoạt động

Blockchain hoạt động theo quy trình sau:

1. Người dùng tạo một giao dịch hoặc yêu cầu lưu trữ dữ liệu.
2. Giao dịch được gửi đến mạng lưới các Node.
3. Các Node kiểm tra tính hợp lệ của giao dịch bằng các thuật toán và cơ chế đồng thuận.
4. Khi giao dịch được xác nhận, nó sẽ được đưa vào một khối mới.
5. Khối mới được gắn với chuỗi Blockchain thông qua mã băm.
6. Tất cả các Node trong mạng đồng thời cập nhật bản sao Blockchain mới nhất.

Nhờ cơ chế này, mọi thành viên trong mạng đều có cùng một bản ghi dữ liệu, giúp hạn chế gian lận và tăng tính minh bạch.

3.4. Đặc điểm nổi bật

Blockchain sở hữu nhiều đặc điểm quan trọng:

- **Phi tập trung:** Không cần một tổ chức trung gian quản lý dữ liệu.
- **Minh bạch:** Mọi giao dịch đều được ghi nhận và có thể kiểm tra.
- **Bảo mật cao:** Dữ liệu được bảo vệ bằng thuật toán mã hóa và cơ chế đồng thuận.
- **Không thể chỉnh sửa tùy ý:** Dữ liệu sau khi xác nhận rất khó bị thay đổi.
- **Khả năng truy xuất nguồn gốc:** Có thể theo dõi lịch sử của mọi giao dịch từ khi được tạo ra.

3.5. Ưu điểm và hạn chế

Ưu điểm

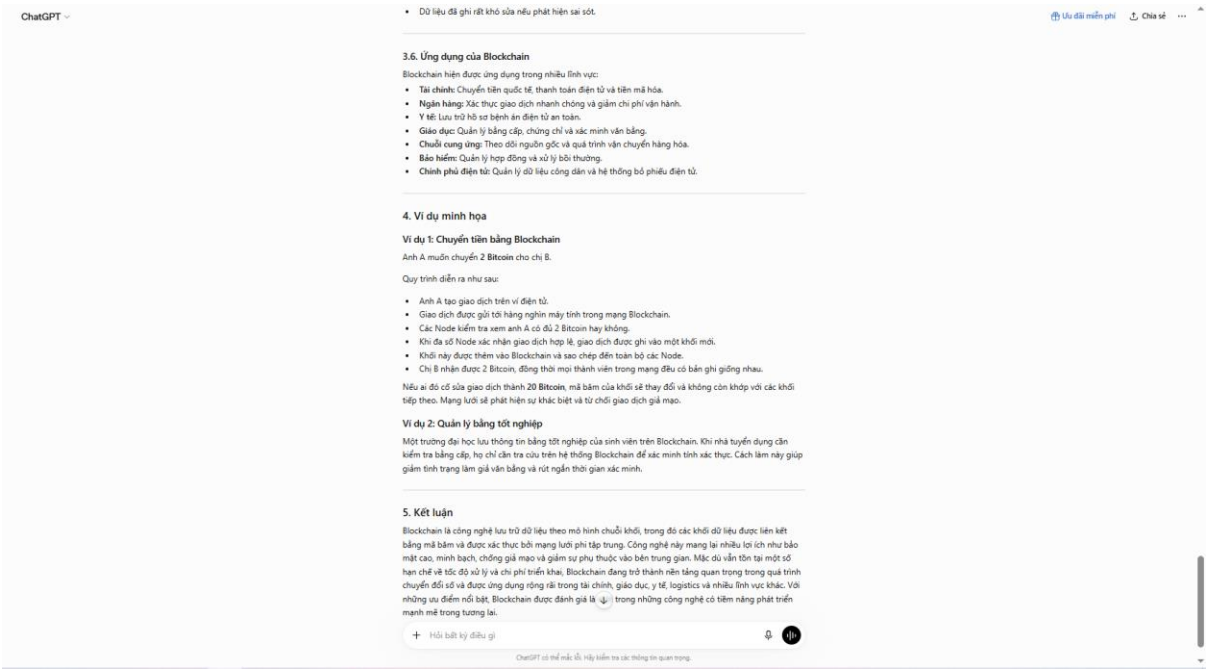
- Bảo mật và an toàn cao.
- Giảm nguy cơ giả mạo dữ liệu.
- Không cần bên trung gian để xác nhận giao dịch.
- Minh bạch, dễ kiểm tra và truy xuất.
- Tăng độ tin cậy giữa các bên tham gia.

Hạn chế

- Tốc độ xử lý giao dịch của một số Blockchain có [illegible]ấm.
- Một số cơ chế đồng thuận tiêu tốn nhiều điện năng và tài nguyên.

Hỏi bất kỳ điều gì

ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.



Prompt nâng cao

Bạn là sinh viên đại học. Thực hiện nhiệm vụ theo từng mục rõ ràng, có ví dụ, giải thích, trình bày dạng bullet, độ dài phù hợp.

Bạn là sinh viên đại học. Thực hiện nhiệm vụ theo từng mục rõ ràng, có ví dụ, giải
thích, trình bày dạng bullet, độ dài phù hợp.

Giải thích Blockchain

1. Đối tượng người đọc

- Sinh viên đại học (đặc biệt các ngành Công nghệ thông tin, Hệ thống thông tin, Thương mại điện tử, Kinh tế số).
- Người mới bắt đầu tìm hiểu về Blockchain.
- Người đọc chưa có kiến thức chuyên sâu về lập trình hoặc mật mã học.

---

2. Độ dài

- Khoảng **700–900 từ**.
- Trình bày ngắn gọn nhưng đầy đủ các nội dung cơ bản.
- Phù hợp đưa vào bài tiểu luận, báo cáo hoặc bài tập học phần.

---

3. Giải thích Blockchain

3.1. Khái niệm

- **Blockchain (chuỗi khối)** là công nghệ lưu trữ dữ liệu dưới dạng các khối (Block) được liên kết với nhau bằng **mã băm (Hash)** theo trình tự thời gian.
- Mỗi khối chứa dữ liệu và được kết nối với khối trước đó, tạo thành một chuỗi liên tục.
- Sau khi dữ liệu được ghi vào Blockchain và được mạng lưới xác nhận, việc sửa đổi hoặc xóa dữ liệu gần như không thể thực hiện.
- Blockchain hoạt động theo mô hình **phi tập trung (Decentralized)**, nghĩa là dữ liệu không do một cá nhân hay tổ chức duy nhất quản lý mà được lưu trên nhiều máy tính (Node) trong mạng.

Giải thích đơn giản:

- Có thể hình dung Blockchain giống như một cuốn sổ ghi chép chung.
- Mỗi người tham gia đều giữ một bản sao giống hệt nhau.
- Khi có thông tin mới, tất cả mọi người cùng xác nhận trước khi ghi vào sổ.
- Vì mọi người đều có bản sao nên rất khó để một cá nhân tự ý sửa nội dung.

3.2. Cấu trúc của Blockchain

Một khối (Block) thường gồm ba thành phần chính:

- **Data (Dữ liệu):**
  - Chứa thông tin cần lưu trữ.
  - Ví dụ: thông tin giao dịch, hợp đồng hoặc hồ sơ.
- **Hash (Mã băm):**
  - Là chuỗi ký tự được tạo bằng thuật toán mã hóa.
  - Đóng vai trò như "dấu vân tay" của khối.
  - Mỗi khối có một Hash riêng và không trùng lặp.
- **Previous Hash (Mã băm của khối trước):**
  - Liên kết khối hiện tại với khối đứng trước.
  - Giúp tạo thành chuỗi dữ liệu liên tục.

Ví dụ minh họa:

- Khối 1
  - Data: A chuyển 1 Bitcoin cho B
  - Hash: XYZ123
- Khối 2
  - Data: B chuyển 0,5 Bitcoin cho C
  - Previous Hash: XYZ123
  - Hash: ABC456

Nếu ai đó sửa dữ liệu trong Khối 1 thì Hash của Khối 1 sẽ thay đổi, dẫn đến Previous Hash của Khối 2 không còn khớp. Hệ thống sẽ phát hiện ngay dữ liệu đã bị can thiệp.

3.3. Nguyên lý hoạt động

Blockchain hoạt động theo các bước sau:

- **Bước 1:** Người dùng tạo một giao dịch.
- **Bước 2:** Giao dịch được gửi đến mạng lưới các Node.
- **Bước 3:** Các Node kiểm tra tính hợp lệ của giao dịch.
- **Bước 4:** Nếu hợp lệ, giao dịch được đưa vào một Block mới.
- **Bước 5:** Block mới được thêm vào Blockchain.
- **Bước 6:** Toàn bộ Node cập nhật bản sao dữ liệu mới.

Ví dụ:

Anh A chuyển **2 Bitcoin** cho chị B.

Quá trình diễn ra như sau:

- Anh A gửi yêu cầu chuyển tiền.
- Hàng nghìn máy tính trong mạng cùng kiểm tra giao dịch.
- Sau khi giao dịch được xác nhận, hệ thống tạo một Block mới.
- Block được thêm vào Blockchain.

Hỏi bất kỳ điều gì

ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.

ChatGPT

Ưu đãi miễn phí Chia sẻ

3.2. Cấu trúc của Blockchain

Một khối (Block) thường gồm ba thành phần chính:

- Data (Dữ liệu):
  - Chứa thông tin cần lưu trữ.
  - Ví dụ: thông tin giao dịch, hợp đồng hoặc hồ sơ.
- Hash (Mã băm):
  - Là chuỗi ký tự được tạo bằng thuật toán mã hóa.
  - Đóng vai trò như "dấu vân tay" của khối.
  - Mỗi khối có một Hash riêng và không trùng lặp.
- Previous Hash (Mã băm của khối trước):
  - Liên kết khối hiện tại với khối đứng trước.
  - Giúp tạo thành chuỗi dữ liệu liên tục.

Ví dụ minh họa:

- Khối 1
  - Data: A chuyển 1 Bitcoin cho B
  - Hash: XYZ123
- Khối 2
  - Data: B chuyển 0,5 Bitcoin cho C
  - Previous Hash: XYZ123
  - Hash: ABC456

Nếu ai đó sửa dữ liệu trong Khối 1 thì Hash của Khối 1 sẽ thay đổi, dẫn đến Previous Hash của Khối 2 không còn khớp. Hệ thống sẽ phát hiện ngay dữ liệu đã bị can thiệp.

3.3. Nguyên lý hoạt động

Blockchain hoạt động theo các bước sau:

- Bước 1: Người dùng tạo một giao dịch.
- Bước 2: Giao dịch được gửi đến mạng lưới các Node.
- Bước 3: Các Node kiểm tra tính hợp lệ của giao dịch.
- Bước 4: Nếu hợp lệ, giao dịch được đưa vào một Block mới.
- Bước 5: Block mới được thêm vào Blockchain.
- Bước 6: Toàn bộ Node cập nhật bản sao dữ liệu mới.

Ví dụ:

Anh A chuyển 2 Bitcoin cho chị B.

Quá trình diễn ra như sau:

- Anh A gửi yêu cầu chuyển tiền.
- Hàng nghìn máy tính trong mạng cùng kiểm tra giao dịch.
- Sau khi giao dịch được xác nhận, hệ thống tạo một Block mới.
- Block được thêm vào Blockchain.

Hỏi bất kỳ điều gì

ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.

- **Bước 1:** Người dùng tạo một giao dịch.
- **Bước 2:** Giao dịch được gửi đến mạng lưới các Node.
- **Bước 3:** Các Node kiểm tra tính hợp lệ của giao dịch.
- **Bước 4:** Nếu hợp lệ, giao dịch được đưa vào một Block mới.
- **Bước 5:** Block mới được thêm vào Blockchain.
- **Bước 6:** Toàn bộ Node cập nhật bản sao dữ liệu mới.

Ví dụ:

Anh A chuyển **2 Bitcoin** cho chị B.

Quá trình diễn ra như sau:

- Anh A gửi yêu cầu chuyển tiền.
- Hàng nghìn máy tính trong mạng cùng kiểm tra giao dịch.
- Sau khi giao dịch được xác nhận, hệ thống tạo một Block mới.
- Block được thêm vào Blockchain.
- Chị B nhận được 2 Bitcoin và mọi máy tính đều lưu lại giao dịch này.

3.4. Đặc điểm nổi bật

Blockchain có nhiều đặc điểm quan trọng:

- **Phi tập trung**
  - Không phụ thuộc vào một máy chủ hoặc tổ chức trung gian.
  - Giảm nguy cơ hệ thống bị tê liệt nếu một máy chủ gặp sự cố.
- **Minh bạch**
  - Lịch sử giao dịch được lưu trữ đầy đủ.
  - Người tham gia có thể kiểm tra thông tin khi cần.
- **Bảo mật cao**
  - Dữ liệu được mã hóa bằng thuật toán Hash.
  - Muốn thay đổi dữ liệu phải thay đổi toàn bộ chuỗi và được đa số mạng chấp nhận, điều này gần như không khả thi.
- **Khó giả mạo**
  - Mọi thay đổi đều để lại dấu vết.
  - Hệ thống nhanh chóng phát hiện dữ liệu bất thường.

3.5. Ưu điểm và hạn chế

Ưu điểm

- Bảo mật tốt.
- Minh bạch và dễ kiểm tra.
- Không cần bên trung gian xác nhận giao dịch.
- Giảm nguy cơ gian lận.
- Dữ liệu được lưu trên nhiều máy nên khó bị mất.

Hạn chế

ChatGPT
Ưu đãi miễn phí
Chia sẻ

- Không cần bên trung gian xác nhận giao dịch.
- Giảm nguy cơ gian lận.
- Dữ liệu được lưu trên nhiều máy nên khó bị mất.

Hạn chế

- Tốc độ xử lý giao dịch có thể chậm hơn cơ sở dữ liệu truyền thống.
- Một số Blockchain tiêu tốn nhiều điện năng.
- Chi phí triển khai ban đầu cao.
- Dữ liệu đã ghi rất khó chỉnh sửa nếu nhập sai.

3.6. Ứng dụng thực tế

Blockchain đang được sử dụng trong nhiều lĩnh vực:

- **Tài chính**
  - Chuyển tiền quốc tế.
  - Thanh toán trực tuyến.
  - Tiền mã hóa.
- **Ngân hàng**
  - Xác minh giao dịch nhanh hơn.
  - Giảm chi phí xử lý.
- **Y tế**
  - Lưu trữ hồ sơ bệnh án.
  - Bảo vệ thông tin bệnh nhân.
- **Giáo dục**
  - Quản lý bằng tốt nghiệp.
  - Xác minh chứng chỉ.
- **Chuỗi cung ứng**
  - Theo dõi nguồn gốc hàng hóa.
  - Kiểm tra quá trình vận chuyển.

Ví dụ:

Một trường đại học lưu bằng tốt nghiệp trên Blockchain.

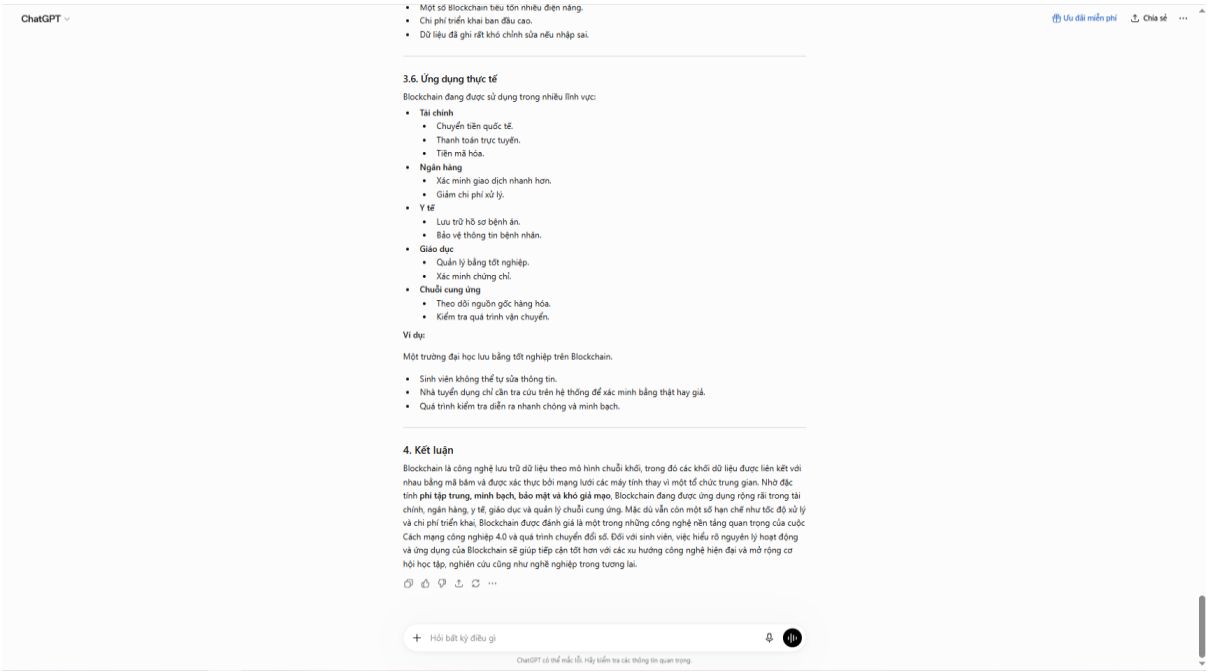
- Sinh viên không thể tự sửa thông tin.
- Nhà tuyển dụng chỉ cần tra cứu trên hệ thống để xác minh bằng thật hay giả.
- Quá trình kiểm tra diễn ra nhanh chóng và minh bạch.

---

4. Kết luận

Blockchain là công nghệ lưu trữ dữ liệu theo mô hình chuỗi khối, trong đó các khối dữ liệu được liên kết với nhau bằng mã băm và được xác thực bởi mạng lưới các máy tính thay vì một tổ chức trung gian. Nhờ đặc tính **phi tập trung**, **minh bạch**, **bảo mật** và **khó giả mạo**, Blockchain đang được ứng dụng rộng rãi trong tài chính, ngân hàng, y tế, giáo dục và quản lý chuỗi cung ứng. Mặc dù vẫn còn một số hạn chế như tốc độ xử lý và chi phí triển khai, Blockchain được đánh giá là một trong những công nghệ nền tảng quan trọng của cuộc Cách mạng công nghiệp 4.0 và quá trình chuyển đổi số. Đối với sinh viên, việc hiểu rõ nguyên lý hoạt động và

Hỏi bất kỳ điều gì
ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.



So sánh kết quả

Tiêu chí	Cơ bản	Cải tiến	Nâng cao
Độ đầy đủ	Thấp	Khá	Rất tốt
Cấu trúc	Ít	Rõ	Rất rõ
Ví dụ	Không	Có	Có nhiều
Khả năng áp dụng	TB	Tốt	Rất tốt

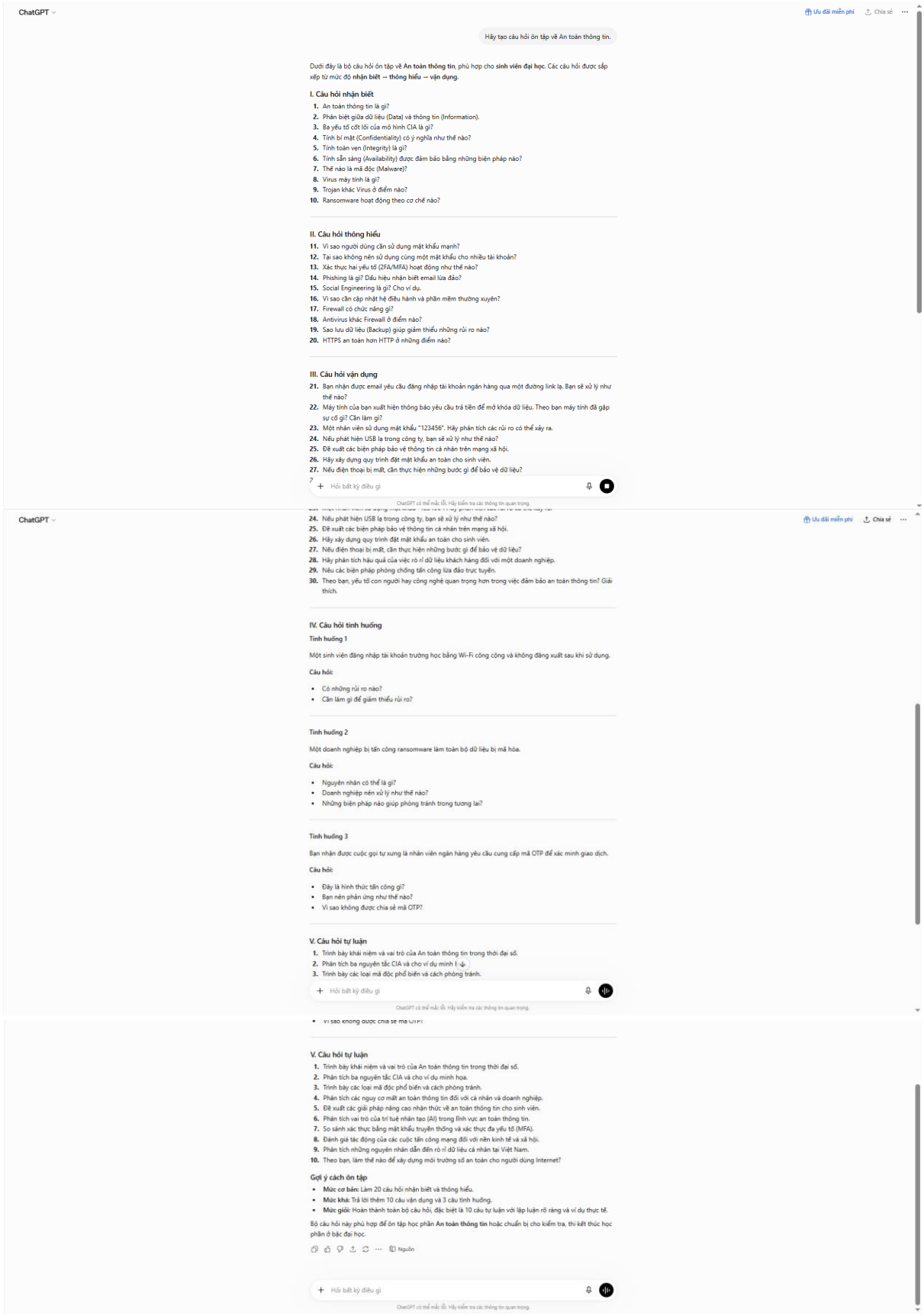
Nhận xét: Prompt nâng cao cho kết quả tốt nhất nhờ cung cấp đầy đủ bối cảnh, vai trò, định dạng và yêu cầu cụ thể.

4. Tạo bộ câu hỏi ôn tập

Mục tiêu: tạo bộ câu hỏi ôn tập về chủ đề An toàn thông tin.

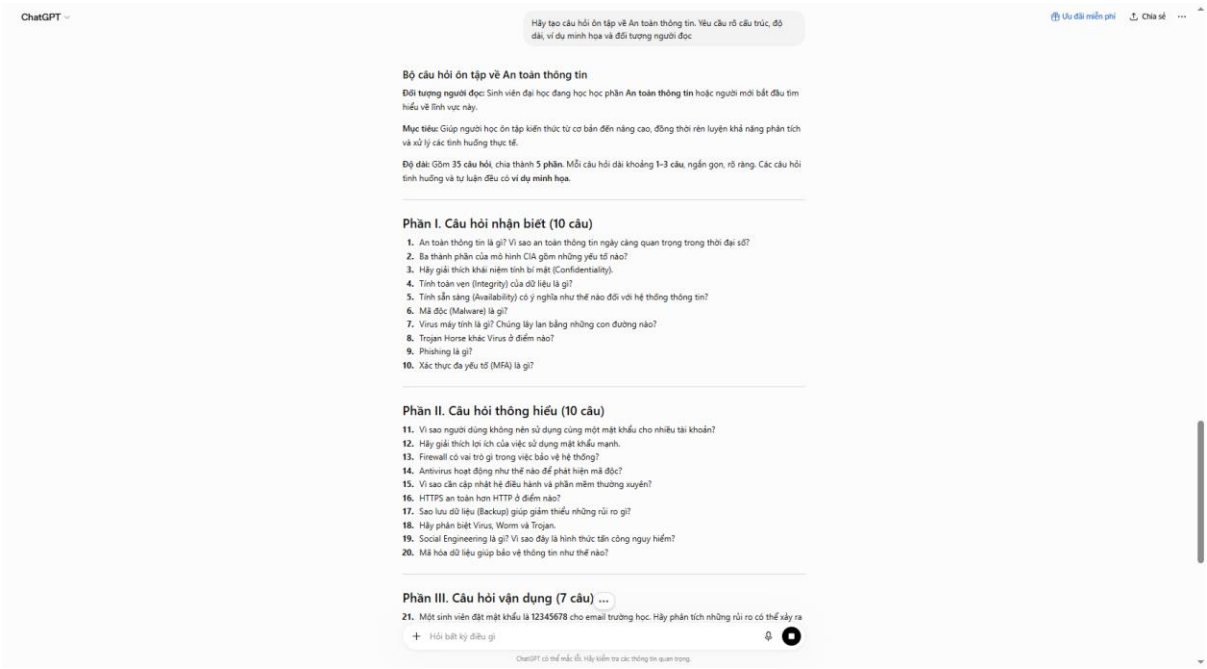
Prompt cơ bản

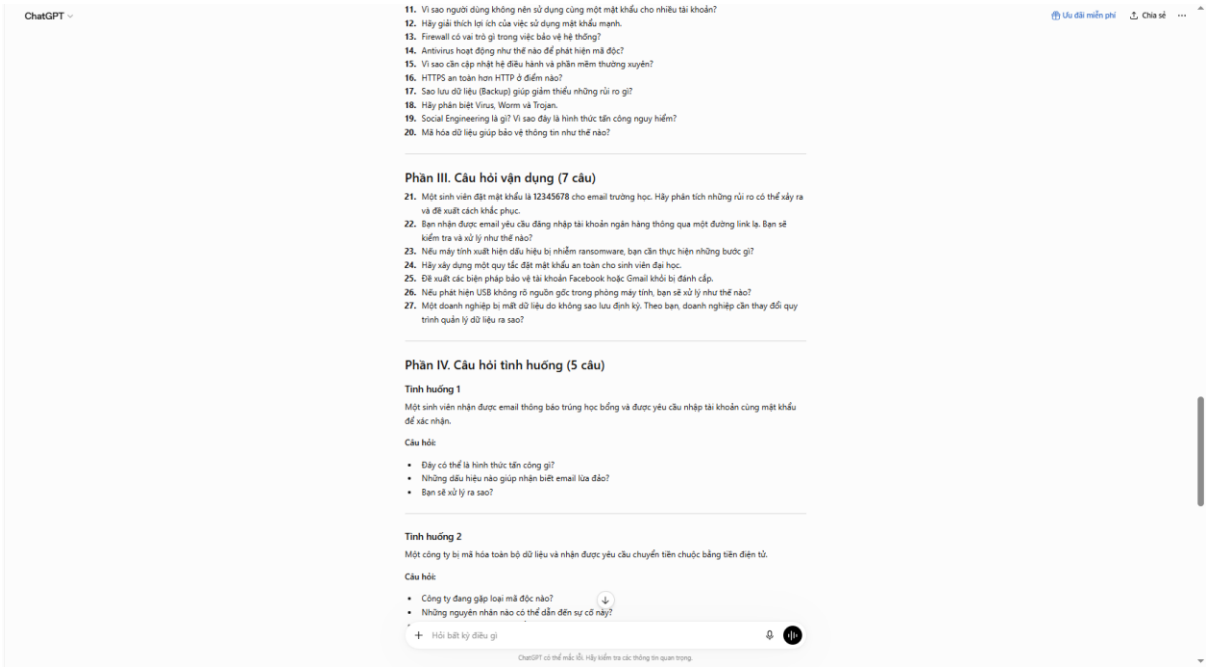
Hãy tạo câu hỏi ôn tập về An toàn thông tin.

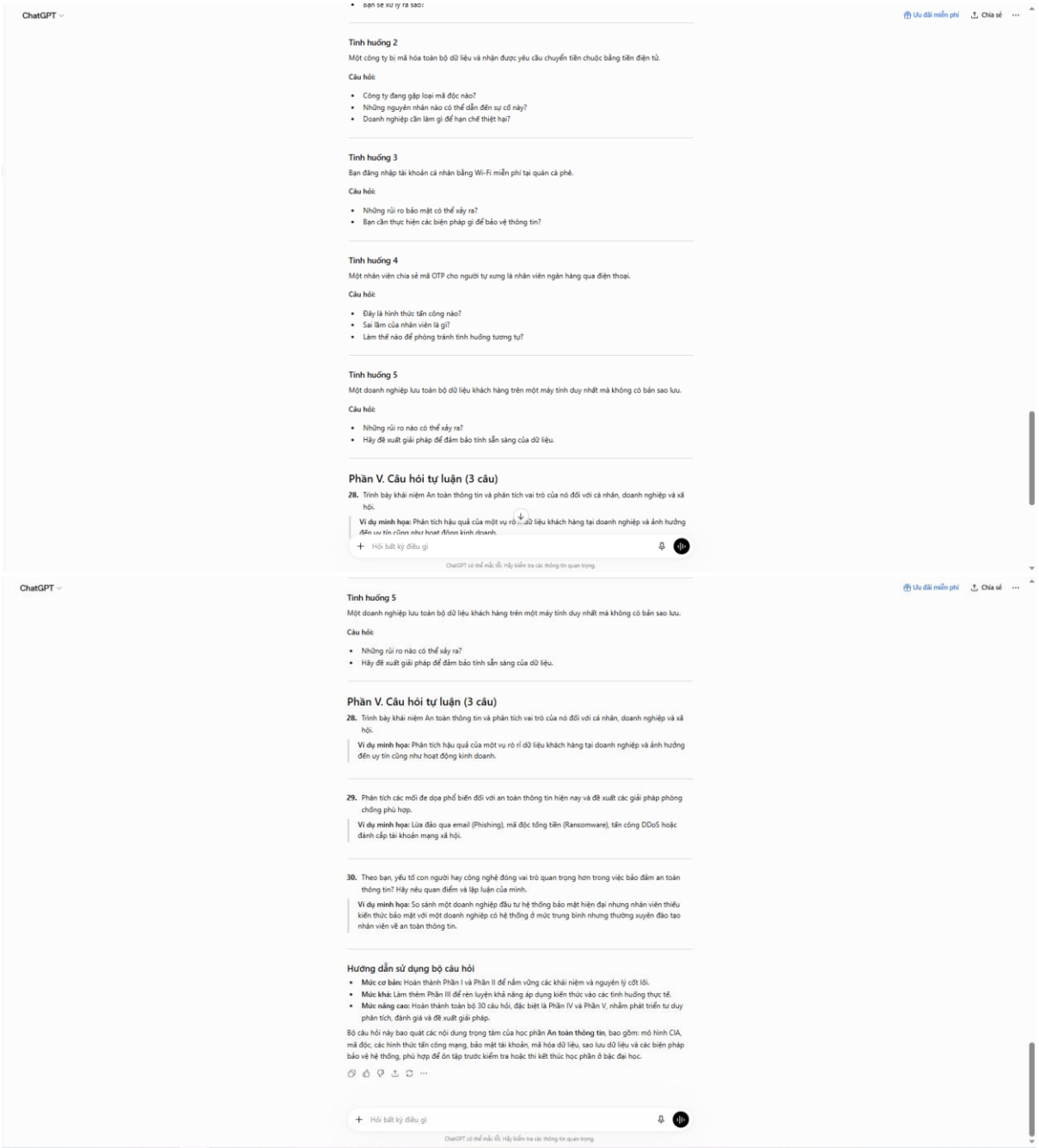


Prompt cải tiến

Yêu cầu rõ cấu trúc, độ dài, ví dụ minh họa và đối tượng người đọc.







Prompt nâng cao

Bạn là sinh viên đại học. Thực hiện nhiệm vụ theo từng mục rõ ràng, có ví dụ, giải thích, trình bày dạng bullet, độ dài phù hợp.

Bạn là sinh viên đại học. Thực hiện nhiệm vụ theo từng mục rõ ràng, có ví dụ, giải thích, trình bày dạng bullet, độ dài phù hợp.

Bộ câu hỏi ôn tập về An toàn thông tin

Đối tượng người đọc: Sinh viên đại học đang học học phần **An toàn thông tin.**

Mục tiêu: Ôn tập kiến thức từ cơ bản đến nâng cao, rèn luyện tư duy phân tích và khả năng vận dụng vào các tình huống thực tế.

Cấu trúc:

- Phần I: Câu hỏi nhận biết
- Phần II: Câu hỏi thông hiểu
- Phần III: Câu hỏi vận dụng
- Phần IV: Câu hỏi tình huống
- Phần V: Câu hỏi tự luận

Độ dài: 30 câu hỏi, mỗi câu dài khoảng 1–3 câu, trình bày ngắn gọn, rõ ràng.

I. Câu hỏi nhận biết (10 câu)

1. An toàn thông tin là gì?
- **Yêu cầu:** Trình bày khái niệm An toàn thông tin.
- **Gợi ý:** Đề cập đến mục tiêu bảo vệ dữ liệu khỏi truy cập, thay đổi hoặc phá hủy trái phép.

2. Mô hình CIA gồm những thành phần nào?
- **Yêu cầu:** Kể tên và nêu ý nghĩa của ba thành phần trong mô hình CIA.
- **Ví dụ:** Một ngân hàng cần đảm bảo dữ liệu khách hàng luôn bí mật, chính xác và có thể truy cập khi cần.

3. Confidentiality (Tính bí mật) là gì?
- **Yêu cầu:** Giải thích khái niệm và nêu một biện pháp giúp đảm bảo tính bí mật.

4. Integrity (Tính toàn vẹn) là gì?
- **Yêu cầu:** Cho biết vì sao dữ liệu cần được đảm bảo tính toàn vẹn.

Hỏi bất kỳ điều gì

ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.

ChatGPT
Ưu đãi miễn phí
Chia sẻ

4. Integrity (Tính toàn vẹn) là gì?
- **Yêu cầu:** Cho biết vì sao dữ liệu cần được đảm bảo tính toàn vẹn.

5. Availability (Tính sẵn sàng) là gì?
- **Yêu cầu:** Nêu ví dụ về hệ thống cần đảm bảo tính sẵn sàng 24/7.

6. Malware là gì?
- **Yêu cầu:** Trình bày khái niệm và nêu ít nhất ba loại mã độc phổ biến.

7. Virus máy tính là gì?
- **Yêu cầu:** Nêu đặc điểm và cách Virus lây lan.

8. Phishing là gì?
- **Yêu cầu:** Giải thích hình thức lừa đảo qua email hoặc website giả mạo.

9. Firewall là gì?
- **Yêu cầu:** Trình bày chức năng chính của Firewall.

10. Xác thực đa yếu tố (MFA) là gì?
- **Yêu cầu:** Giải thích nguyên lý hoạt động của MFA.

II. Câu hỏi thông hiểu (8 câu)

11. Vì sao cần sử dụng mật khẩu mạnh?
- **Yêu cầu:** Phân tích lợi ích của mật khẩu mạnh.
- **Ví dụ:** So sánh mật khẩu **123456** với **Abc@2026#Secure.**

12. Vì sao không nên dùng chung một mật khẩu cho nhiều tài khoản?
- **Yêu cầu:** Phân tích những rủi ro có thể xảy ra.

13. Phân biệt Virus, Worm và Trojan.
- **Yêu cầu:** So sánh về cách lây lan và mức độ nguy hiểm.

Hỏi bất kỳ điều gì

ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.

13. Phân biệt Virus, Worm và Trojan.

- **Yêu cầu:** So sánh về cách lây lan và mức độ nguy hiểm.

14. HTTPS khác HTTP như thế nào?

- **Yêu cầu:** Giải thích vai trò của chứng chỉ SSL/TLS.

15. Vì sao cần cập nhật phần mềm thường xuyên?

- **Yêu cầu:** Giải thích mối liên hệ giữa bản vá bảo mật và an toàn thông tin.

16. Sao lưu dữ liệu (Backup) có vai trò gì?

- **Yêu cầu:** Trình bày các lợi ích khi thực hiện sao lưu định kỳ.

17. Social Engineering là gì?

- **Yêu cầu:** Giải thích vì sao con người thường là mắt xích yếu nhất trong bảo mật.

18. Antivirus và Firewall khác nhau như thế nào?

- **Yêu cầu:** So sánh chức năng của hai công cụ.

III. Câu hỏi vận dụng (5 câu)

19. Tình huống sử dụng mật khẩu yếu

Một sinh viên đặt mật khẩu Gmail là **123456789**.

Yêu cầu

- Phân tích các nguy cơ có thể xảy ra.
- Đề xuất cách đặt mật khẩu an toàn hơn.

20. Tình huống email giả mạo

Bạn nhận được email thông báo tài khoản ngân hàng sắp bị khóa và yêu cầu đăng nhập qua một đường link.

Yêu cầu

Hỏi bất kỳ điều gì
ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.

ChatGPT
Ưu đãi miễn phí
Chia sẻ

- Đề xuất cách đặt mật khẩu an toàn hơn.

20. Tình huống email giả mạo

Bạn nhận được email thông báo tài khoản ngân hàng sắp bị khóa và yêu cầu đăng nhập qua một đường link.

Yêu cầu

- Xác định dấu hiệu bất thường.
- Nêu các bước xử lý phù hợp.

21. Tình huống mất điện thoại

Điện thoại lưu tài khoản Facebook, Gmail và ứng dụng ngân hàng bị mất.

Yêu cầu

- Liệt kê các bước cần thực hiện để giảm thiểu thiệt hại.

22. Tình huống USB lạ

Bạn nhìn thấy một USB không rõ nguồn gốc trong phòng máy.

Yêu cầu

- Bạn sẽ xử lý như thế nào?
- Giải thích lý do.

23. Tình huống ransomware

Máy tính cá nhân không thể mở được các tệp và xuất hiện yêu cầu trả tiền chuộc.

Yêu cầu

- Xác định nguyên nhân.
- Đề xuất các bước xử lý.

IV. Câu hỏi tình huống (4 câu)

Tình huống 1

Một doanh nghiệp bị rò rỉ thông tin khách hàng sau khi nhân viên mở tệp đính kèm trong email lạ.

Câu hỏi

Hỏi bất kỳ điều gì
ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.

- Đề xuất các bước xử lý.

IV. Câu hỏi tình huống (4 câu)

Tình huống 1

Một doanh nghiệp bị rò rỉ thông tin khách hàng sau khi nhân viên mở tệp đính kèm trong email lạ.

Câu hỏi

- Nguyên nhân của sự cố là gì?
- Doanh nghiệp cần làm gì để khắc phục?
- Làm thế nào để phòng tránh sự cố tương tự?

Ví dụ minh họa

- Email giả mạo có tiêu đề **"Hóa đơn tháng này"** nhưng chứa mã độc.

Tình huống 2

Một sinh viên thường xuyên đăng nhập Facebook bằng Wi-Fi miễn phí tại quán cà phê.

Câu hỏi

- Những nguy cơ bảo mật có thể xảy ra?
- Đề xuất các biện pháp bảo vệ.

Ví dụ minh họa

- Hacker tạo điểm phát Wi-Fi giả để đánh cắp thông tin đăng nhập.

Tình huống 3

Một nhân viên chia sẻ mã OTP cho người gọi điện tự xưng là nhân viên ngân hàng.

Câu hỏi

- Đây là hình thức tấn công gì?
- Sai lầm của nhân viên là gì?
- Cách phòng tránh?

Ví dụ minh họa

- Kẻ gian sử dụng kỹ thuật **Social Engineering** để lấy OTP.

Tình huống 4

Một doanh nghiệp không sao lưu dữ liệu trong nhiều tháng. Sau khi máy chủ gặp sự cố, toàn bộ dữ liệu bị mất.

Câu hỏi

Hỏi bất kỳ điều gì
ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.

ChatGPT
Ưu đãi miễn phí
Chia sẻ

- Những hậu quả có thể xảy ra?
- Đề xuất quy trình sao lưu phù hợp.

Ví dụ minh họa

- Thực hiện sao lưu tự động mỗi ngày và lưu thêm một bản trên dịch vụ đám mây.

V. Câu hỏi tự luận (3 câu)

28. Phân tích vai trò của An toàn thông tin trong thời đại chuyển đổi số.

Yêu cầu

- Trình bày khái niệm.
- Phân tích vai trò đối với:
  - Cá nhân.
  - Doanh nghiệp.
  - Cơ quan nhà nước.
- Đưa ra ví dụ minh họa thực tế.

Độ dài gợi ý: 500–700 từ.

29. Phân tích các mối đe dọa an toàn thông tin phổ biến hiện nay.

Yêu cầu

- Trình bày các loại tấn công:
  - Phishing.
  - Ransomware.
  - DDoS.
  - Malware.
  - Social Engineering.
- Đề xuất biện pháp phòng chống tương ứng.

Ví dụ minh họa

- Một doanh nghiệp bị ransomware do nhân viên tải tệp từ nguồn không đáng tin cậy.

Độ dài gợi ý: 600–800 từ.

30. Theo bạn, yếu tố con người hay công nghệ quan trọng hơn trong việc đảm bảo an toàn thông tin?

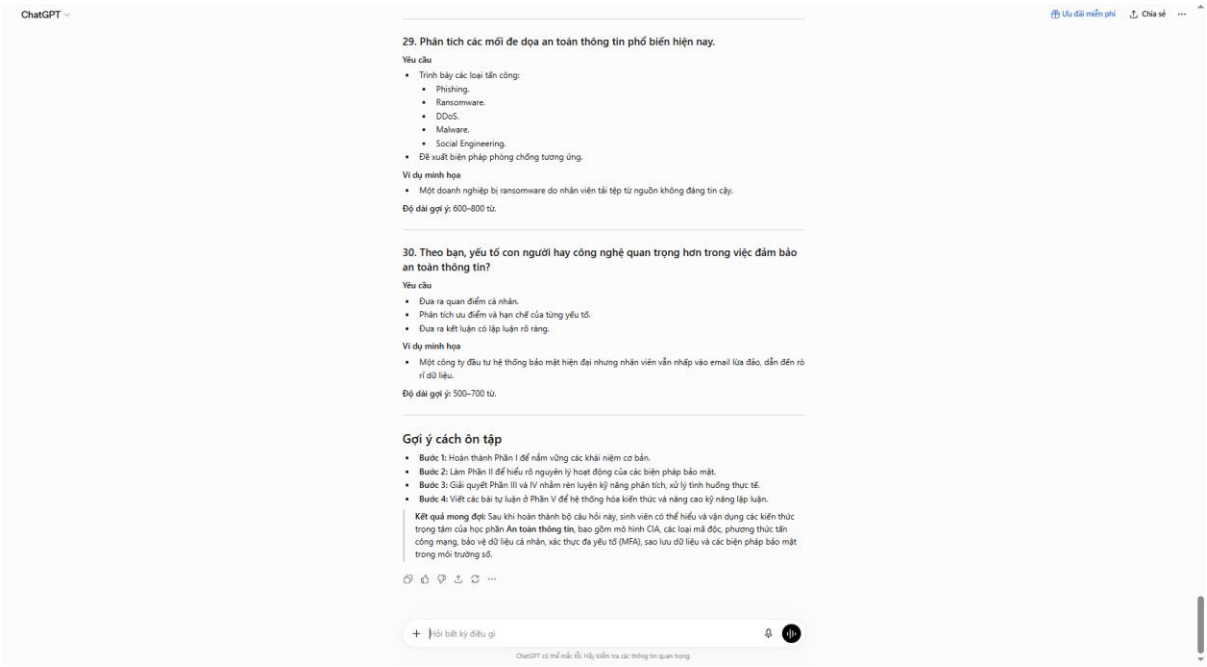
Yêu cầu

- Đưa ra quan điểm cá nhân.
- Phân tích ưu điểm và hạn chế của từng yếu tố.
- Đưa ra kết luận có lập luận rõ ràng.

Ví dụ minh họa

- Một công ty đầu tư hệ thống bảo mật hiện đại nhưng nhân viên vẫn nhấp vào email lừa đảo, dẫn đến rò

Hỏi bất kỳ điều gì
ChatGPT có thể mắc lỗi. Hãy kiểm tra các thông tin quan trọng.



So sánh kết quả

Tiêu chí	Cơ bản	Cải tiến	Nâng cao
Độ đầy đủ	Thấp	Khá	Rất tốt
Cấu trúc	Ít	Rõ	Rất rõ
Ví dụ	Không	Có	Có nhiều
Khả năng áp dụng	TB	Tốt	Rất tốt

Nhận xét: Prompt nâng cao cho kết quả tốt nhất nhờ cung cấp đầy đủ bối cảnh, vai trò, định dạng và yêu cầu cụ thể.

5. Phân tích vì sao prompt nâng cao hiệu quả

Prompt nâng cao hiệu quả hơn vì xác định rõ vai trò của AI (role prompting), nêu đầy đủ mục tiêu, quy định định dạng đầu ra, giới hạn độ dài, yêu cầu ví dụ và chia nhỏ nhiệm vụ. Điều này giúp AI hiểu đúng yêu cầu, giảm câu trả lời lan man và tăng tính nhất quán.

6. Nguyên tắc viết prompt hiệu quả

· Xác định mục tiêu rõ ràng.

· Cung cấp bối cảnh.

· Chỉ định vai trò của AI.

· Quy định định dạng đầu ra.

· Nêu giới hạn độ dài.

· Yêu cầu ví dụ minh họa.

· Chia nhiệm vụ thành từng bước.

· Thử nghiệm và cải tiến prompt nhiều lần.

7. Kết luận

Qua thử nghiệm có thể thấy chất lượng prompt ảnh hưởng trực tiếp đến chất lượng câu trả lời của AI. Prompt càng cụ thể, có cấu trúc và đầy đủ bối cảnh thì kết quả càng chính xác và hữu ích.