A text on a page

Description automatically generated

Câu 1: Ý tưởng kinh doanh cho nhóm này có thể là tạo ra các dịch vụ cao cấp liên quan đến nhu cầu của cộng đồng học thuật trên website. Ví dụ, nhóm có thể cung cấp các dịch vụ sau:

1. **Khuyến mãi và Quảng cáo**: Họ có thể thu hút các nhà tài trợ, tổ chức, hoặc doanh nghiệp muốn tiếp cận cộng đồng học thuật thông qua quảng cáo hoặc tài trợ nội dung.
2. **Dịch vụ Tạo Nội Dung Chất Lượng**: Nhóm có thể cung cấp dịch vụ tạo nội dung chuyên sâu, nghiên cứu hoặc phân tích đối với các tổ chức hoặc cá nhân muốn chia sẻ thông tin trên nền tảng của họ.
3. **Khóa học trực tuyến và Sự kiện Thực tế**: Họ có thể tổ chức các khóa học trực tuyến hoặc sự kiện học thuật đặc biệt mà người dùng có thể trả phí để tham gia.
4. **Dịch vụ Tư vấn Học thuật**: Nhóm có thể cung cấp dịch vụ tư vấn hoặc hỗ trợ cho cá nhân hoặc tổ chức về các vấn đề liên quan đến nghiên cứu, viết bài, hoặc phát triển nghề nghiệp trong lĩnh vực học thuật.

Câu 2: Mô hình kinh doanh Canvas cho ý tưởng kinh doanh trên:

1. Khách hàng:

- Cộng đồng học thuật, sinh viên, giáo viên, nhà nghiên cứu, các tổ chức nghiên cứu, doanh nghiệp quan tâm đến học thuật.

2. Đề xuất Giá trị:

- Nền tảng trao đổi học thuật phong phú và đa dạng.

- Dịch vụ tạo nội dung chất lượng.

- Cơ hội học tập và kết nối với người chuyên môn trong các lĩnh vực khác nhau.

3. Kênh phân phối:

- Website và ứng dụng di động.

- Quảng cáo trực tuyến.

- Hợp tác với các tổ chức học thuật và doanh nghiệp.

4. Mối quan hệ với khách hàng:

- Tương tác trực tuyến qua nền tảng.

- Hỗ trợ trực tuyến.

- Tổ chức sự kiện và khóa học offline.

9. Cơ cấu chi phí:

- Phát triển và duy trì nền tảng công nghệ.

- Chi phí tiếp thị và quảng cáo.

- Chi phí hoạt động và hỗ trợ khách hàng.

5. Doanh thu:

- Doanh thu từ quảng cáo và tài trợ.

- Doanh thu từ bán các dịch vụ tạo nội dung và học thuật.

- Doanh thu từ bán khóa học và sự kiện.

7. Tài nguyên chìa khóa:

- Nền tảng website và ứng dụng.

- Nội dung học thuật chất lượng và người dùng tích cực.

- Đội ngũ phát triển công nghệ và hỗ trợ khách hàng.

6. nguồn lực chính

8. đối tác chính

Câu 3: Mối đe dọa về an ninh mạng cho mỗi tài sản:

* **Website**:
  + Tấn công DDoS có thể làm cho trang web trở nên không hoạt động.
  + Tấn công SQL Injection hoặc Cross-Site Scripting (XSS) có thể dẫn đến lỗ hổng bảo mật và đánh cắp thông tin người dùng hoặc dữ liệu quan trọng.
  + Rủi ro về vi phạm bản quyền hoặc vi phạm quyền riêng tư khi người dùng chia sẻ thông tin không được bảo vệ.
* **User profile**:
  + Mối đe dọa về vi phạm quyền riêng tư khi thông tin người dùng bị tiết lộ hoặc sử dụng không đúng mục đích.
  + Rủi ro về các cuộc tấn công phishing nhằm vào thông tin cá nhân của người dùng.

Câu 4: Đề xuất các biện pháp bảo vệ, phát hiện, ứng phó và khắc phục cho mối đe dọa đối với website đã xác định ở câu 3:

* **Bảo vệ**:
  + Sử dụng các dịch vụ bảo mật mạng như Cloudflare để chống lại tấn công DDoS.
  + Thiết lập các giới hạn truy cập và kiểm soát lưu lượng mạng để ngăn chặn tấn công từ nguồn không xác định.
* **Phát hiện**:
  + Sử dụng hệ thống giám sát mạng và ghi lại các biểu hiện của tấn công DDoS như sự tăng đột ngột trong lưu lượng mạng.
* **Ứng phó**:
  + Tự động kích hoạt các biện pháp phòng ngừa khi phát hiện có dấu hiệu của tấn công DDoS, như chuyển hướng lưu lượng mạng qua các bộ lọc.

A document with text and images

Description automatically generated with medium confidence

Câu 1: Ý tưởng kinh doanh cho nhóm này có thể là tạo ra một hệ thống đánh giá và đảm bảo chất lượng cho các dịch vụ giúp việc được cung cấp thông qua website. Ví dụ:

1. **Dịch vụ Đánh giá và Xác thực**: Cung cấp dịch vụ kiểm tra và xác minh thông tin của người giúp việc, đảm bảo họ đáp ứng các tiêu chuẩn an toàn và chất lượng.
2. **Dịch vụ Đào tạo và Phát triển**: Cung cấp các khóa đào tạo và hướng dẫn cho người giúp việc nhằm nâng cao kỹ năng và hiểu biết.
3. **Dịch vụ Hỗ trợ và Tư vấn**: Cung cấp dịch vụ tư vấn và hỗ trợ cho các gia đình và người giúp việc để giải quyết các vấn đề phát sinh trong quá trình làm việc.

Câu 2: Mô hình kinh doanh Canvas cho ý tưởng kinh doanh trên:

1. Khách hàng:

- Gia đình cần tìm người giúp việc.

- Người giúp việc muốn tìm công việc.

2. Đề xuất Giá trị:

- Dịch vụ giúp việc nhà chất lượng và tin cậy.

- Hỗ trợ và tư vấn cho cả gia đình và người giúp việc.

- Hệ thống đánh giá và xác thực người giúp việc.

3. Kênh phân phối:

- Website và ứng dụng di động.

- Quảng cáo trực tuyến.

- Hợp tác với các cộng đồng trực tuyến và tổ chức phi lợi nhuận.

4. Mối quan hệ với khách hàng:

- Tương tác trực tuyến qua nền tảng.

- Phản hồi và hỗ trợ khách hàng.

- Tổ chức sự kiện và hoạt động giao lưu cộng đồng.

5. Cơ cấu chi phí:

- Phát triển và duy trì nền tảng công nghệ.

- Chi phí tiếp thị và quảng cáo.

- Chi phí đào tạo và xác thực người giúp việc.

6. Doanh thu:

- Phí dịch vụ từ việc kết nối gia đình với người giúp việc.

- Doanh thu từ dịch vụ đào tạo và tư vấn.

- Doanh thu từ quảng cáo và hợp tác đối tác.

7. Tài nguyên chìa khóa:

- Nền tảng website và ứng dụng.

- Dữ liệu và lý lịch của người giúp việc.

- Đội ngũ phát triển công nghệ và hỗ trợ khách hàng.

Câu 3: Mối đe dọa về an ninh mạng cho mỗi tài sản:

* **Website**:
  + Tấn công hacking hoặc phá hoại gây mất dữ liệu hoặc làm hỏng website.
  + Rủi ro về vi phạm quyền riêng tư khi thông tin cá nhân của khách hàng và người giúp việc bị tiết lộ.
* **CSDL lý lịch của người giúp việc**:
  + Nguy cơ bị tấn công để đánh cắp thông tin cá nhân hoặc sử dụng sai mục đích.
  + Rủi ro về việc dữ liệu bị thay đổi hoặc làm giả để lừa đảo.

Câu 4: Đề xuất các biện pháp bảo vệ, phát hiện, ứng phó và khắc phục cho mối đe dọa đối với CSDL lý lịch của người giúp việc:

* **Bảo vệ**:
  + Sử dụng mã hóa dữ liệu để bảo vệ thông tin lý lịch của người giúp việc.
  + Thiết lập các cơ chế kiểm soát truy cập để chỉ cho phép người có quyền truy cập vào dữ liệu.
* **Phát hiện**:
  + Sử dụng hệ thống giám sát và nhật ký hoạt động để phát hiện các hành vi không bình thường hoặc tấn công vào CSDL.
* **Ứng phó**:
  + Thực hiện sao lưu dữ liệu định kỳ để đảm bảo có thể khôi phục lại thông tin nhanh chóng sau một sự cố.
  + Thực hiện các biện pháp phòng ngừa như việc cập nhật phần mềm và hệ thống bảo mật định kỳ.

**Ý tưởng kinh doanh**

Vấn đề nhóm muốn giải quyết: giảm thiểu ô nhiễm chất thải nhựa. Thay thế ống hút nhựa, cải thiện môi trường sống

**Mô hình Canvas**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **8.Key Parnerships (Đối tác chính)**  - Quảng cáo sản phẩm  - Nhà cung cấp nguyên vật liệu: cung cấp nguyên liệu để sản xuất bánh ngọt  - Đối tác vận chuyển: cung cấp dịch vụ vận chuyển và giao hàng cho khách hàng  - Các trang web  - Công ty thanh toán | **7. Key activities**  **(Hoạt động chính)**  - Marketing thu hút khách hàng  - Thiết kế bao bì sản phẩm  - Thiết kế các loại bánh ngọt và hương vị khác nhau.  - Giải pháp giải quyết các vấn đề an toàn vệ sinh thực phẩm  - Cung cấp sản phẩm đến tay người tiêu dùng  - Tổ chức quản lý đặt hàng bánh ngọt  - Quản lý và kiểm soát chất lượng nguyên liệu và sản phẩm đúng cách. | **2.Value Propositions**  **(Tuyên bố giá trị)**  - Đảm bảo an toàn thực phẩm  - Tiết kiệm thời gian đi lại, có thể cầm nắm dễ dàng  - Giá cả hợp lý phù hợp với từng khách hàng  - Đảm bảo sử dụng nguyên liệu tốt nhất và chất lượng cao nhất để tạo ra các sản phẩm bánh ngọt.  - Cung cấp dịch vụ đặt bánh ngọt cho các sự kiện, sinh nhật,.. | **4.Customer Relationships (Mối quan hệ khách hàng)**  - Hỗ trợ khách hàng tốt, tạo cho khách một trải nghiệm tốt  - Tạo môi trường thân thiện nhiệt tình  - Cung cấp một số thông tin hữu ích cho khách hàng  - Đưa ra cho khách hàng những ưu đãi, khuyến mãi về sản phẩm  - Tích điểm cho khách hàng quen thuộc  - Tích hợp công nghệ để khách hàng thuận tiện mua hàng | **1. Customer Segments** (Phân khúc khách hàng)  - Giới trẻ  - Những người ăn kiêng, béo phì  - Khách hàng bán sỉ  - Các buổi tiệc cho doanh nghiệp, sinh nhật hoặc sự kiện  - Các chuỗi cà phê, nhà hàng, khách sạn |
| **6. Key Resources (Nguồn lực chính)**  - Có nguồn liệu chính: bột mì, đường, bơ, trứng, sữa,..  - Cơ sở vật chất: lò nướng, máy xay, máy trộn,…  - Giấy an toàn vệ sinh thực phẩm  - Nhân lực: Đầu bếp, nhân viên bán hàng, nhân viên tiếp nhận đơn,…Có kiến thức vè chuyên môn ngành, kỹ năng làm việc nhóm  - Chiến lược quảng bá sản phẩm hiệu quả  - Hệ thống quản lý đặt hàng, giao hàng hiệu quả | **3.Channels (Kênh phân phối)**  - Trên sàn thương mại điện tử (Shopee, Lazada,..)  - Các app như Gojeck, Grapfood, Beamin, Tiktok…  - Cửa hàng bán lẻ |
| **9. Cost Structure (Cơ cấu chi phí)**  - Một số chí phí để vận hành MHKD:   * Chi phí mặt bằng. * Chi phí vận chuyển. * Trả lương cho nhân viên. * Chi phí vận hành máy móc. * Chi phí quảng cáo. * Chi phí mua nguyên liệu. | | | **5. Revenue Streams (Dòng doanh thu)**  **-** Từ các chương trình khuyến mãi.  - Từ các buổi sự kiện, sinh nhật.  - Từ các kênh phân phối.  - Giá bán: Bánh cupcake, Bánh bông lan, Bánh mì ngọt… phụ thuộc vào kích thước của từng loại bánh. Có 3 kích thước chuẩn:  +Size nhỏ: 15.000 đồng mỗi loại  +Size trung: 25.000 đồng mỗi loại  +Size lớn: 45.000 đồng mỗi loại  +Size khách hàng yêu cầu sẽ tăng tùy thuộc vào kích thước bánh (chủ yếu bánh sinh nhật,…) | |

A close-up of a paper

Description automatically generated

Câu a: các phương thức tấn công hacker có thể sử dụng:

* ransomeware: email spam chứa mã độc, các trang web nhiễm virus,…
* Trojan: Ẩn dưới chương trình tiện ích, chờ người dùng tải về
* Dụ dỗ tiết lộ thông tin dưới hình thức ẩn danh
* Đánh cắp laptop, điện thoại, thiết bị có chứa thông tin,…

Câu b:

* ransomeware: email spam chứa mã độc, các trang web nhiễm virus,…, hacker tạo một email có chứa mã độc và gửi tới email của nhân viên, và khi nhân viên nhấn vào email đó thì tiến hành đánh cắp thông tin

Câu c:

* Khóa tài khoản bị đánh cắp
* Kiểm tra các thông tin bị đánh cắp
* Thông tin đến người dùng biết
* Xem xét mức độ nguy hiểm

Câu d:

* Sử dụng phần mềm bảo vệ email: Sử dụng phần mềm bảo vệ email có thể giúp loại bỏ các tệp đính kèm độc hại và chặn các liên kết đến các trang web độc hại.
* Đào tạo nhân viên: Đào tạo nhân viên của bạn về các mối đe dọa bảo mật cơ bản và cách phòng chống chúng có thể giúp giảm thiểu nguy cơ tấn công từ các Class 6 - Vấn đề về an ninh TMDT 7 loại mã độc
* Sao lưu dữ liệu thường xuyên: Tạo bản sao dữ liệu thường xuyên và lưu trữ chúng ở nơi an toàn có thể giúp phục hồi các tài liệu quan trọng nếu hệ thống bị tấn công bởi các loại mã độc.

Câu f:

* Giám sát nhậtj kí
* Thực hiện các quy trình xâm nhập, theo cấp độ mạng và thiết bị
* Cài đặt phần mềm phát hiện xâm nhập bất thường

Câu e:

* Đào tạo nhập viên: vì nhân viên những cá nhân trực tiêp sử dụng các tài khoảng hệ thống
* **Bài tập nhóm chương 3**
* **Mô tả:**
* Một nhóm startup đã xây dựng app và website hỗ trợ học tập. Người dùng có thể thảo luận về kiến thức các môn học, bài tập ứng dụng, chat riêng, hoặc cùng chơi các game phát triển trí não như đánh cờ,…và mua tài liệu tham khảo.
* Văn phòng của công ty ở trong tòa nhà X tại Tp.HCM, hiện có 20 nhân viên. Tất cả các nhân viên đều được cấp thẻ nhân viên để vào tòa nhà, một chiếc iPhone và máy tính xách tay. Tất cả nhân viên đều nhận được email hướng dẫn các giải pháp an ninh mạng, nhưng không phải nhân viên nào cũng đọc hết nội dung trong email. Nhân viên chưa trải qua bất kỳ khóa đào tạo bắt buộc nào về an ninh mạng.
* Gần đây, công ty đã xảy ra một mối đe dọa an ninh mạng. Do đó, họ đang tìm cách cải thiện an ninh mạng và đang tìm kiếm chuyên gia an ninh mạng để giúp đỡ.
* Sự cố an ninh mạng gần đây của công ty:
* Một nhân viên đã để quên máy tính xách tay trên tàu khi đi công tác. Trên máy tính xách tay đã lưu các tài khoản để đăng nhập vào trang quản trị ứng dụng và website của công ty, cơ sở dữ liệu và một số tài liệu của công ty. Nhân viên đã báo mất cho công ty ngay khi phát hiện sự cố, và máy tính xách tay đã bị xóa dữ liệu từ xa. Công ty không thể chắc chắn có dữ liệu nào đã được truy cập trước khi dữ liệu máy tính bị xóa từ xa.
* *Chú ý: Các quy định quan trọng của chính phủ về bảo vệ thông tin cá nhân*
* **Yêu cầu:**
* Nhóm của bạn gồm các chuyên gia an ninh mạng và sẽ phải đề xuất các giải pháp cho các mối đe dọa an ninh mạng của họ.
* Tài sản chính của công ty là gì? Họ cần bảo vệ điều gì? (Tài sản là một hạng mục tài sản thuộc sở hữu của một người hoặc công ty. Đây có thể là tài sản vật chất hoặc thông tin họ nắm giữ). Các biện pháp bảo vệ, phát hiện, ứng phó, khắc phục đối với mỗi mối đe dọa.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tài sản vật chất** | **Các mối đe dọa an ninh mạng tiềm ẩn** | **Bảo vệ** | **Phát hiện** | **Ứng phó** | **Khắc phục** |
| 1) iPhone của công ty cho tất cả nhân viên | - Mất thông tin dữ liệu của công ty khi truy cập vào gmail của điện thoại  - | -Tạo mật khẩu điện thoại  -Bảo mật dữ liệu icloud, đặt mật khẩu icloud  - Thường xuyên sao lưu dữ liệu icloud | - Nhật ký truy cập icloud từ iphone  - Các tài liệu bị truy cập từ iphone | -Xem xét tài khoản icloud có bị truy cập hay không  -Xem các tài liệu trong máy có bị truy cập truy xuất dữ liệu hay không | - Sử dụng các thiết bị khác để đăng xuất tài khoản và xóa tài khoản khỏi iphone |
| 2) Máy tính xách tay | - Mất cơ sở dữ liệu và một số tài liệu của công ty  - Nguy cơ mất website | - Máy tính phải có mật khẩu  - Bảo mật dữ liệu có trong máy, đặt tườnglửa,mật khẩu cho dữ liệu nhậy cảm trong máy  -Tạo bản full bakup cho dữ liệu và thông tin quan trọng trong máy | -Phát hiện truy cập lạ, truy xuất dữ liệu bất thường kích hoạt cảnh báo cho người dùng máy | -Xác định và vô hiệu hóa nguồn gây hại ngay lập tức  -Sử dụng phần mềm bảo mật để bảo vệ dữ liệu nhạy cảm  -Mã hóa các dữ liệu quan trọng | -Restore các dữ liệu đã backup  -Sửa chữa và phục hồi thiết bị bị tấn công  -Cập nhật phần mềm thường xuyên để bảo vệ máy |
| 3)… |  |  |  |  |  |
| … |  |  |  |  |  |
|  |  |  |  |  |  |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Tài sản thông tin** | **Các mối đe dọa an ninh mạng tiềm ẩn** | **Bảo vệ** | **Phát hiện** | **Ứng phó** | **Khắc phục** |
| 1) Thông tin cá nhân của khách hàng | -Mất thông tin của khách hàng | -Mã hóa dữ liệu quan trọng của khách hàng  -Tạo bản full bakup cho dữ liệu và thông tin quan trọng của khách hàng | -Thông tin của khách hàng bị truy cập từ nguồn lạ  -Thông tin của khách hàng bị truy xuất bất thường | -Kích hoạt hệ thống bảo mật bảo vệ thông tin  -Mã hóa các dữ liệu quan trọng ngay lập tức  -Ngăn chặn các truy cập, truy xuất dữ liệu lạ, bất thường từ nguồn lạ | -Restore các dữ liệu đã backup  -Thông báo với khách hàng về các hoạt động phản hồi và phục hồi dữ liệu |
| 2) Thẻ nhân viên | -Mất thông tin của nhân viên | -Mã hóa các dữ liệu quan trọng của nhân viên  -Tạo bản full bakup cho dữ liệu và thông tin quan trọng của nhân viên | -Phát hiện thông tin của Nhân viên bị truy cập và truy xuất từ các nguồn lạ một cách bất thường | -Kích hoạt hệ thống bảo mật bảo vệ thông tin  -Mã hóa các dữ liệu quan trọng ngay lập tức  -Ngăn chặn các truy cập, truy xuất dữ liệu lạ, bất thường từ nguồn lạ | -Restore các dữ liệu đã backup  -Thông báo với nhân viên về các hoạt động phản hồi và phục hồi dữ liệu |
|  |  |  |  |  |  |