

LIÊN HIỆP CÁC HỘI KHOA HỌC KỸ THUẬT VIỆT NAM  
CUỘC THI SÁNG TẠO DÀNH CHO THANH THIẾU NIÊN,  
NHÌ ĐỒNG TOÀN QUỐC LẦN THỨ 21 (NĂM 2025)

NĂM HỌC 2024-2025

# BÁO CÁO KẾT QUẢ NGHIÊN CỨU

TÊN DỰ ÁN:

PHÒNG CHỐNG LỪA ĐẢO TRÊN  
KHÔNG GIAN MẠNG - ANTI SCAM

LĨNH VỰC DỰ THI:

PHẦN MỀM TIN HỌC

133.876 DATA

EXTENSION TIỆN LỢI

TIN CẬY - UY TÍN- AN TOÀN

BLOG CÔNG NGHỆ

HỖ TRỢ NÂNG CAO KIẾN THỨC AN TOÀN MẠNG

ĐƠN GIẢN DỄ SỬ DỤNG

Mã QR đường dẫn dự án



Là nơi lưu trữ bằng chứng lừa đảo, cung cấp góp phần nào thúc đẩy  
quá trình thu thập dữ liệu phục vụ cho công tác điều tra của “Cục An  
ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao”

## Mục lục

<b>I. Câu hỏi hay vấn đề đặt ra</b>	
1. Thực trạng hiện nay .....	Trang 3
2. Vấn đề về công nghệ.....	Trang 4
3. Nghiên cứu bắt đầu dự án .....	Trang 4
<b>II. Mục tiêu kết quả mong đợi</b>	
1. Trang web Phòng chống lừa đảo trên không gian mạng-ANTI SCAM ..	Trang 5
2. Tổng thể về dự án .....	Trang 6
<b>III. Giả thuyết khoa học và những điều Phòng chống lừa đảo trên không gian mạng ANTI SCAM đã làm được</b>	
1. Giả thuyết khoa học .....	Trang 7
2. Những điều Phòng chống lừa đảo trên không gian mạng-ANTI SCAM đã làm được .....	Trang 7
<b>IV. Phạm vi nghiên cứu</b>	
1. Phạm vi về loại hình lừa đảo trên không gian mạng .....	Trang 10
2. Phạm vi đối tượng người dùng .....	Trang 11
3. Phạm vi nghiên cứu về công nghệ và giải pháp kỹ thuật .....	Trang 11
4. Phạm vi nghiên cứu về giáo dục và nâng cao nhận thức .....	Trang 11
5. Phạm vi nghiên cứu về pháp lý và các chính sách.....	Trang 11
6. Phạm vi nghiên cứu về các cơ chế hỗ trợ và giám sát .....	Trang 11
7. Phạm vi về khu vực nghiên cứu.....	Trang 12
<b>V. Kế hoạch nghiên cứu và chuẩn bị thực hiện</b>	
1. Kế hoạch .....	Trang 12
2. Chuẩn bị .....	Trang 13
3. Thực hiện .....	Trang 13
<b>VI. Thành tựu số liệu nghiên cứu.....</b>	Trang 14
<b>VII. Kết luận.....</b>	Trang 14
<b>VIII. Nguồn tham khảo .....</b>	Trang 15

Quét mã để xem báo cáo điện tử:



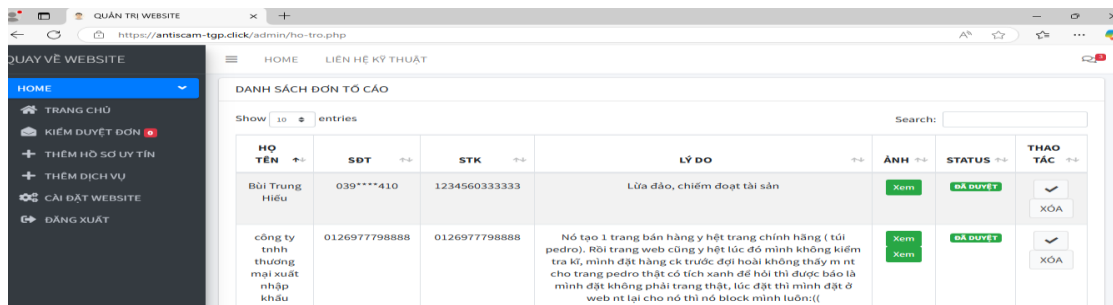
Tiện ích khi sử dụng báo cáo điện tử:

- ✓ Ban giám khảo có thể tiết kiệm thời gian khi thao tác trực tiếp.
- ✓ Báo cáo được trình bày đẹp mắt đồ họa cao.



**Chú thích:** để vào xem phần “Quản lý trang tố cáo lừa đảo” của Phòng chống lừa đảo trên không gian mạng-ANTISCAM. Thầy/cô cần phải đăng nhập vào trang web với tài khoản và mật khẩu sau:

- Trang web: <https://antiscam-tgp.click/admin/login.php>
- Tài khoản đăng nhập: admin
- Mật khẩu: Admin@2024



## THÔNG TIN WEBSITE

**Trang chủ:** <https://antiscam-tgp.click/>

**Trang thông tin:** <https://antiscam-tgp.click/blog/>

- Phiên bản 1.0.0
- Tác giả: Trần Gia Phú.
- Thông tin mã nguồn: Php, Nodejs, Css, MySQL, HTML, Javascrip.
- Phiên bản Website: Donet Blazor.
- Thông tin mã nguồn – máy chủ:
  - Máy chủ: H2Cloud (NET CORE 8)
  - Cơ sở dữ liệu: MySQL

## **TÓM TẮT DỰ ÁN**

### **“PHÒNG CHỐNG LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG-ANTI SCAM”**

#### **I. Câu hỏi hay vấn đề đặt ra:**

##### **1. Thực trạng hiện nay.**

Ngày nay, chúng ta đang bước vào kỷ nguyên của nền kinh tế tri thức, trong đó khoa học và công nghệ đã trở thành lực lượng sản xuất chủ yếu. Sản phẩm của khoa học và công nghệ chiếm phần lớn trong giá trị của nhiều hàng hóa, dịch vụ. Khoa học công nghệ đang tạo ra sự khác biệt to lớn trong sự phát triển giữa các quốc gia, trong đó phải kể đến những thành tựu vượt bậc của công nghệ thông tin và truyền thông. Tuy nhiên, bên cạnh những thành tựu do khoa học công nghệ đem lại, còn những mặt trái mà chúng ta không mong muốn đó là khoa học công nghệ được sử dụng vào nhiều hoạt động phạm tội và được thế giới gọi chung là “*Tội phạm sử dụng công nghệ cao*”. Đây là loại tội phạm mới, đang có xu hướng phát triển, đa dạng, diễn biến hết sức phức tạp và khó lường trên quy mô toàn cầu, đe dọa đến sự ổn định, phát triển của các quốc gia và tạo ra thách thức lớn cho mỗi quốc gia.

Theo thống kê của Bộ Thông tin và Truyền thông, hiện nay nước ta có khoảng 31,5 triệu người sử dụng mạng Internet (chiếm 1/3 dân số cả nước), internet băng rộng đạt 12 triệu thuê bao (trong đó: Băng thông rộng cố định đạt 7 triệu thuê bao, băng thông rộng di động 3G/4G đạt gần 5 triệu thuê bao); điện thoại di động đạt 138 triệu thuê bao. Về ứng dụng công nghệ thông tin, 100% cơ quan Nhà nước có trang, cổng thông tin điện tử, cung cấp hơn 100.000 dịch vụ công trực tuyến các loại phục vụ người dân và doanh nghiệp. Tội phạm sử dụng công nghệ cao tại Việt Nam đã lợi dụng triệt để tính ưu việt của mạng internet để thực hiện hành vi phạm tội, gây ra nhiều hậu quả xấu đối với xã hội.

##### **\* Các loại hình tấn công phổ biến:**

– **Tấn công deface:** Truy cập bất hợp pháp vào cơ sở dữ liệu nhằm phá hoại, sửa đổi dữ liệu, trộm cắp dữ liệu và thay đổi giao diện.

– **Tấn công từ chối dịch vụ DDoS:** Làm tắc nghẽn đường truyền bằng cách cài mã điều khiển các máy tính "ma" trong mạng botnet truy cập liên tục và lặp đi lặp lại vào một địa chỉ trang web đã định trước.

– **Phát tán virus, phần mềm gián điệp:** Phát tán qua dịch vụ Web 2.0 như Yume, Second Life, Facebook, Flickr, YouTube, Anhsos, ... nhằm lây lan vào máy tính cá nhân để lấy thông tin cá nhân như mật khẩu của E-mail, tài khoản Chat.

– **Tội phạm trong thương mại điện tử:** Lừa đảo qua quảng cáo, bán hàng trực tuyến; lừa trên các sàn giao dịch ảo như ngoại tệ, vàng, bất động sản, huy động vốn tín dụng; lừa đảo bằng E-mail từ các nước châu Phi, châu Âu thông báo trúng thưởng xổ số lớn, đề nghị tham gia rửa tiền, đề nghị nhận hộ tiền thừa kế, ...

– **Thủ đoạn rút tiền từ thẻ ngân hàng:** Thông đồng với nơi chấp nhận thẻ để rút tiền; mua hàng qua mạng bằng thông tin thẻ trộm cắp; rửa tiền với nhiều loại tiền ảo như

Liberty Reserve, e-Gold, Paypal, Webmoney, ePassport...; chuyển tiền từ thẻ tín dụng trộm cấp sang tài khoản ngân hàng; dùng thẻ tín dụng trộm cấp để đánh bạc, cá độ qua mạng.

– **Lừa đảo trong mua bán hàng qua mạng-B2B:** Khi ký hợp đồng qua mạng, đặc biệt là hợp đồng ngoại thương, tội phạm thường thực hiện đúng hợp đồng đầu để tạo lòng tin. Khi lượng tiền thanh toán lên đến hàng triệu USD, đối tượng nhanh chóng rút tiền trước khi người mua phát hiện hành vi lừa đảo và không giao hàng hoặc giao hàng không đúng hợp đồng.

➤ *Từ thực trạng nêu trên, tôi đã lập trình thiết kế ra Website để: Là nơi lưu trữ bằng chứng lừa đảo, giúp cho người dùng kiểm tra được tài khoản, những hồ sơ lừa đảo trên không gian mạng. Cung cấp, nâng cao được kiến thức trên môi trường không gian mạng cho mọi người.*

## 2. Vấn đề về công nghệ:

Công nghệ nói chung và công nghệ thông tin nói riêng đang ngày càng phát triển với tốc độ nhanh chóng. Hiện nay các công nghệ đang được nghiên cứu và sử dụng với các đối tượng có tính chuyên môn cao chưa bình dân hóa.

Các lập trình viên ngày càng phải làm nhiều công việc. Nhưng đối với công việc lập trình hiện tại gần như chỉ hỗ trợ trên các thiết bị máy tính bàn, laptop, ... nhưng trong thời đại công nghệ đang phát triển nhanh chóng đòi hỏi công cụ hỗ trợ có thể hoạt động trên chính trên cả 2 thiết bị máy tính và điện thoại di động thông minh.

Các bạn học sinh, sinh viên, các lập trình viên, ... với số vốn nhỏ và có kiến thức chuyên môn về công nghệ phần mềm muốn tạo một dự án “khởi nghiệp” riêng cho bản thân. Với số vốn nhỏ hầu như không thể cạnh tranh đưa lên các sàn như CH Play, App Store, ... và quảng cáo sản phẩm ứng dụng của mình đến với nhiều người dùng.

Bên cạnh đó vấn nạn của xã hội hiện nay là lừa đảo trên không gian mạng ngày càng phổ biến. Vì vậy, cần có giải pháp cấp thiết để giải quyết vấn nạn nêu trên, tôi đã đưa ra ý tưởng thiết kế Trang Web phòng chống lừa đảo trên không gian mạng-AntiScam (<https://antiscam-tgp.click/>) đã được lên kế hoạch, xây dựng và phát triển.

## 3. Nghiên cứu bắt đầu dự án:

Từ vấn đề “công cụ tìm kiếm, kiểm tra và tri thức” và “công nghệ” em bắt đầu nghiên cứu thực hiện dự án “**PHÒNG CHỐNG LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG- ANTI SCAM**” với ý nghĩa “*Là nơi lưu trữ bằng chứng lừa đảo, giúp cho người dùng kiểm tra được tài khoản, những hồ sơ lừa đảo trên không gian mạng. Cung cấp, nâng cao được kiến thức trên môi trường không gian mạng cho mọi người*”.

Để thực hiện hai vấn đề trên và đảm bảo tính hiệu quả và phát triển của **PHÒNG CHỐNG LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG- ANTI SCAM**, nên em đã nghiên cứu, lập nên dự án và phân tích chi tiết:

- Tìm kiếm, kiểm tra và tố cáo lừa đảo, thống kê.
- Cung cấp giải pháp công nghệ
- Quản lý trang

## II. Mục tiêu kết quả mong đợi

### 1. Trang web Phòng chống lừa đảo trên không gian mạng- ANTI SCAM

– **Mục tiêu thứ nhất:** Nâng cao **nhận thức** cộng đồng về các **hình thức** lừa đảo trên không gian mạng

Cung cấp thông tin chi tiết về các loại lừa đảo trực tuyến phổ biến như lừa đảo qua email, mạng xã hội, gian lận tài chính trực tuyến, và các hình thức lừa đảo khác.

Cung cấp các cảnh báo và tin tức cập nhật về các mối đe dọa lừa đảo mới.

– **Mục tiêu thứ hai:** Cung cấp các **hướng dẫn** và **biện pháp phòng ngừa** cho người dùng

Hướng dẫn người dùng cách nhận diện các dấu hiệu của lừa đảo trực tuyến.

Đưa ra các lời khuyên về cách bảo mật thông tin cá nhân và tài khoản trực tuyến.

Cung cấp các phương pháp bảo vệ tài khoản email, mạng xã hội, và tài khoản ngân hàng khỏi các mối nguy hiểm trực tuyến.

– **Mục tiêu thứ ba:** Tạo không gian **hỗ trợ** người bị lừa đảo

Cung cấp thông tin về các cơ quan chức năng và tổ chức hỗ trợ người bị lừa đảo.

Tạo một nền tảng để người dùng có thể báo cáo các vụ lừa đảo mà họ gặp phải.

– **Mục tiêu thứ tư:** Cung cấp các **công cụ kiểm tra** và **xác thực** thông tin

Cung cấp các công cụ kiểm tra tính xác thực của email, trang web, hoặc thông tin từ các nguồn không xác định, số điện thoại, tài khoản ngân hàng, ...

Giới thiệu các dịch vụ bảo mật như phần mềm diệt virus, công cụ chống phishing, hay VPN.

– **Mục tiêu thứ năm:** **Hợp tác** với các tổ chức và cơ quan chức năng

Tăng cường sự hợp tác với các cơ quan pháp luật và tổ chức bảo vệ quyền lợi người tiêu dùng để có thể giải quyết hiệu quả các vấn đề lừa đảo.

Đảm bảo việc bảo vệ quyền lợi của người tiêu dùng thông qua việc nâng cao sự phối hợp giữa các bên liên quan.

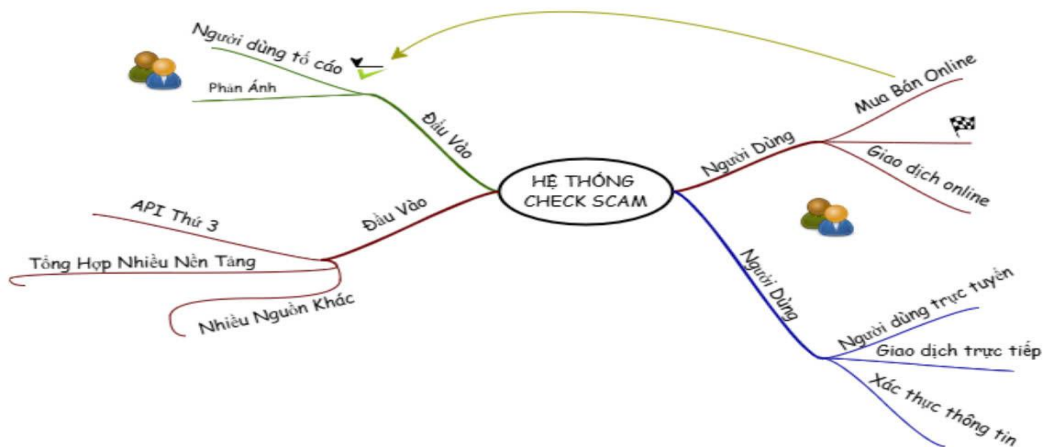
– **Mục tiêu thứ sáu:** Là nơi **lưu trữ** bằng chứng lừa đảo, cung cấp góp phần nào thúc đẩy **quá trình thu thập** dữ liệu phục vụ cho công tác điều tra của “Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao”.

– **Mục tiêu thứ bảy:** **Đào tạo và phát triển** các chương trình **giáo dục** về an toàn mạng. Cung cấp khóa học hoặc chương trình đào tạo về an toàn mạng cho các đối tượng người dùng khác nhau như học sinh, sinh viên, người lao động, và doanh nghiệp.

– **Mục tiêu chung:** Mục tiêu chung của dự án là tạo ra một **nền tảng** thông tin và **hỗ trợ** hiệu quả nhằm bảo vệ người dùng khỏi các mối nguy cơ lừa đảo trên không gian mạng



## 2. Tổng thể về dự án.



**DỰ ÁN PHÒNG CHỐNG LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG - ANTI SCAM** có tham vọng và mục tiêu lớn là trở thành một nền tảng toàn diện và đáng tin cậy, chuyên cung cấp thông tin, công cụ và giải pháp phòng ngừa lừa đảo trực tuyến cho người dùng toàn cầu. Cụ thể, dự án sẽ hướng đến các mục tiêu sau:

- Trở thành nguồn tài nguyên hàng đầu về phòng chống lừa đảo trực tuyến:

Cung cấp kiến thức chuyên sâu và cập nhật về các mối đe dọa lừa đảo trên không gian mạng.

Trở thành một kênh tham khảo uy tín, nơi người dùng có thể tìm thấy các thông tin bảo mật, hướng dẫn phòng tránh lừa đảo và các biện pháp bảo vệ an toàn trên mạng.

- Xây dựng cộng đồng người dùng an toàn trên không gian mạng:

Xây dựng một cộng đồng trực tuyến mạnh mẽ, nơi mọi người có thể chia sẻ kinh nghiệm, báo cáo các vụ lừa đảo và cảnh báo nguy hiểm với nhau.

Tạo dựng môi trường hỗ trợ và giúp đỡ nhau trong việc bảo vệ tài khoản, thông tin cá nhân khỏi các mối đe dọa.

- Cung cấp các công cụ, phần mềm và dịch vụ bảo vệ người dùng hiệu quả:

Phát triển các công cụ kiểm tra, xác thực thông tin, trang web, email, và ứng dụng để giúp người dùng nhận diện và tránh xa các nguy cơ lừa đảo.

Đưa ra các giải pháp bảo mật, phần mềm diệt virus, phần mềm chống phishing, VPN để giúp người dùng an toàn hơn khi trực tuyến.

- Định hướng giáo dục và đào tạo an toàn mạng cho mọi đối tượng:

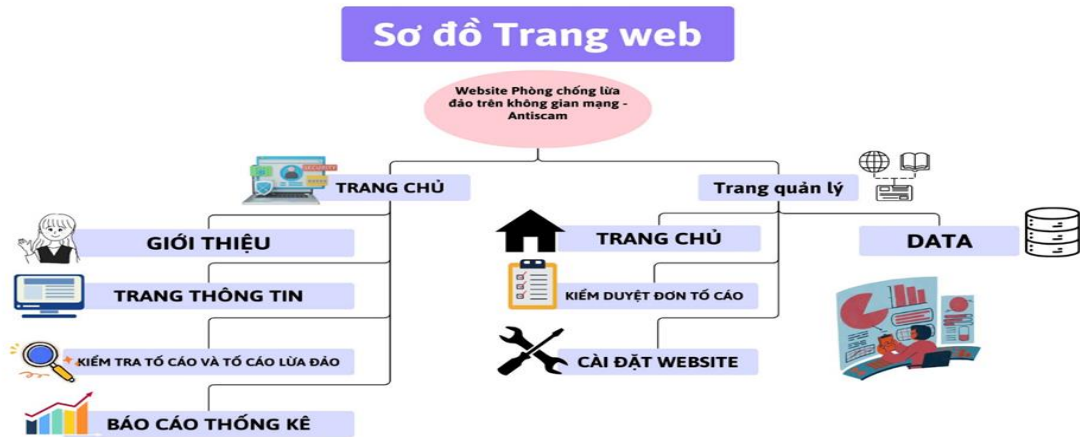
Cung cấp nhận thức về an toàn mạng cho mọi đối tượng từ học sinh, sinh viên, người lao động đến các doanh nghiệp.

Phát triển, trang bị kiến thức cơ bản về phòng tránh lừa đảo cho các nhóm đối tượng dễ bị tổn thương, như nhóm người cao tuổi, trẻ em hoặc người thiếu kinh nghiệm về an ninh mạng có nguy cơ cao bị lừa đảo.

➤ Xây dựng nền tảng toàn cầu phòng chống lừa đảo qua không gian mạng: Mở rộng dự án không chỉ trong phạm vi một quốc gia mà còn trên toàn cầu, để hỗ trợ và bảo vệ người dùng ở mọi quốc gia.

Với các mục tiêu *“Là nơi lưu trữ bằng chứng lừa đảo, giúp cho người dùng kiểm tra được tài khoản, những hồ sơ lừa đảo trên không gian mạng. Cung cấp, nâng cao được kiến*

*thức trên môi trường không gian mạng cho mọi người”, dự án ANTI SCAM sẽ không chỉ giúp ngăn chặn các hành vi lừa đảo, mà còn tạo ra một môi trường mạng an toàn và đáng tin cậy cho người dùng trên toàn thế giới. Chính vì điều đó **DỰ ÁN PHÒNG CHỐNG LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG - ANTI SCAM** đã lập nên những chiến lược mục tiêu nghiên cứu và thực hiện phát triển chặt chẽ và theo quy trình logic. Với nguồn dữ liệu khổng lồ từ nghiên cứu để dễ dàng quản lý và phát triển dự án được phân chia thành các phần như hình ảnh:*



### III. Giả thuyết khoa học và những điều Phòng chống lừa đảo trên không gian mạng- ANTI SCAM đã làm được

#### 1. Giả thuyết khoa học

- Từ vấn đề “công cụ tìm kiếm, kiểm tra và tri thức” đã đặt ra câu hỏi:
  - Câu hỏi về kiểm duyệt nội dung.
  - Câu hỏi xây dựng nền tảng.
- Từ vấn đề “công nghệ” đã đặt ra câu hỏi:
  - Câu hỏi rút gọn chi phí công nghệ bình dân hóa số.
  - Câu hỏi nền tảng lập trình trên cả 2 thiết bị, máy tính và điện thoại di động thông minh.
  - Câu hỏi kho ứng dụng dành cho dự án khởi nghiệp công nghệ.

➤ Từ các câu hỏi vấn đề trên giả thuyết được đặt ra: ***nền tảng nào? dự án nào? người nào? sẽ có thể giải quyết được một phần hoặc tất cả các câu hỏi vấn đề trên.***

#### 2. Những điều Phòng chống lừa đảo trên không gian mạng-ANTI SCAM đã làm được:

##### ❖ Tổng thể dự án

– Về công nghệ: Xây dựng thành công và đi vào *hoạt động thực tế* với 3 trang web chủ chốt, sau thời gian thực hiện nghiên cứu là <https://antiscam-tgp.click/>, <https://antiscam-tgp.click/blog/> và <https://antiscam-tgp.click/admin/login.php>.

– Tổng quan về công nghệ:

• Trang quản lý: <https://antiscam-tgp.click/admin/login.php> [Username: admin, Password: Admin@2024].



QUẢN TRỊ WEBSITE

HOME

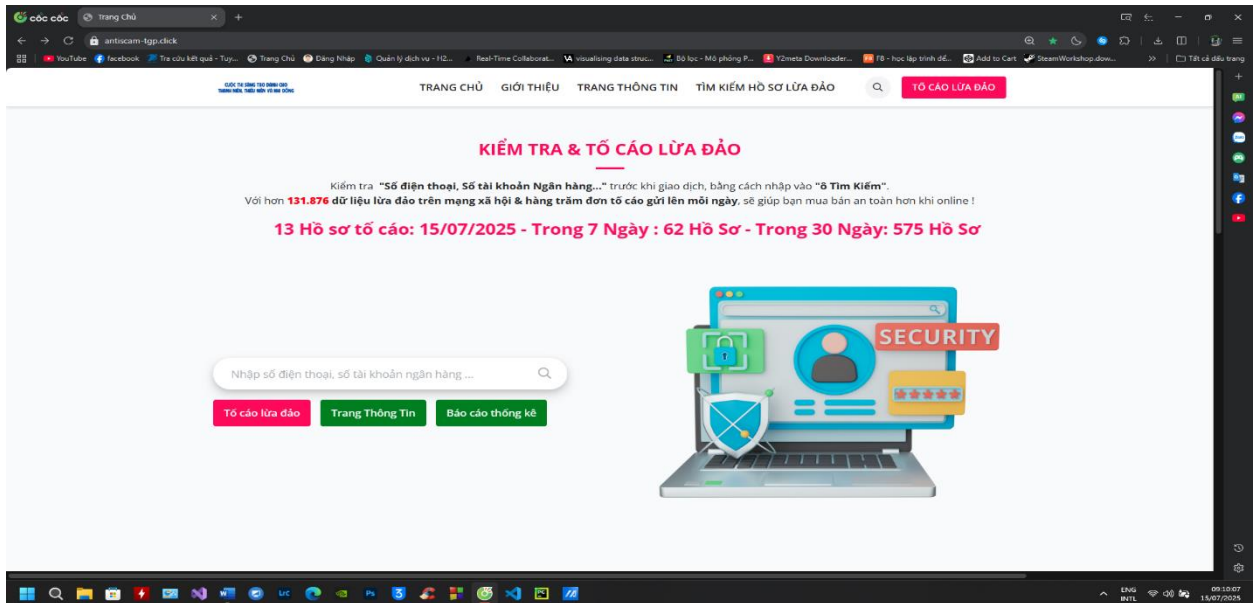
LIÊN HỆ KỸ THUẬT

DANH SÁCH ĐƠN TỐ CÁO

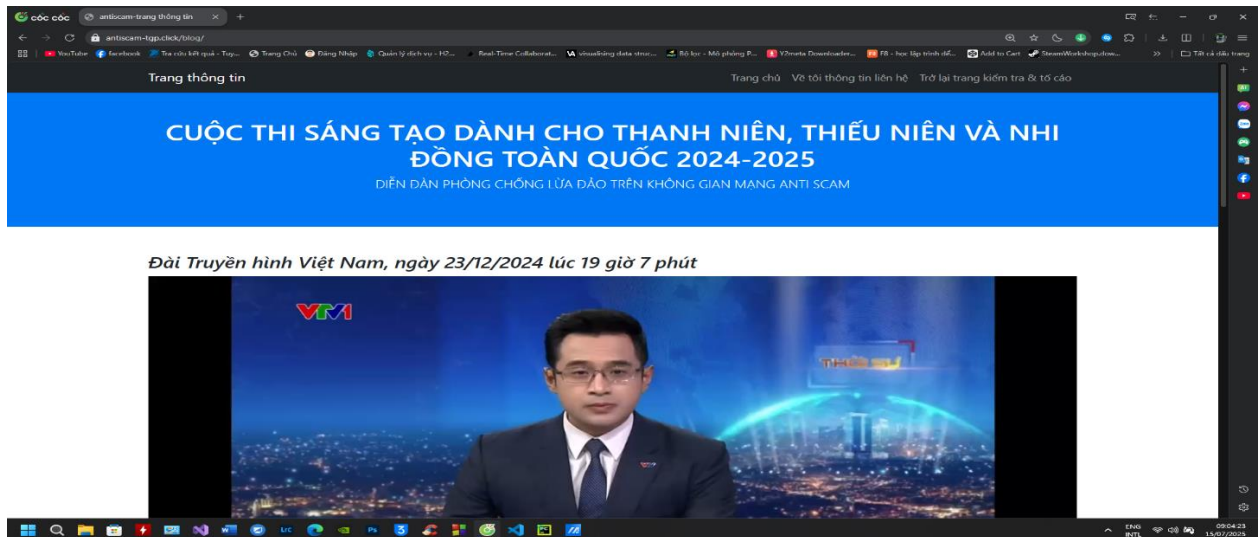
Show 10 entries

HỌ TÊN	SĐT	STK	LÝ DO	ẢNH	STATUS	THAO TÁC
Bùi Trung Hiếu	039****410	1234560333333	Lừa đảo, chiếm đoạt tài sản	Xem	ĐÃ DUYỆT	XÓA
công ty TNHH thương mại xuất nhập khẩu	0126977798888	0126977798888	Nó tạo 1 trang bán hàng y hệt trang chính hãng (túi pedro). Rồi trang web cũng y hệt lúc đó mình không kiểm tra kĩ, mình đặt hàng ck trước đợi hoài không thấy m nt cho trang pedro thật có tích xanh để hỏi thì được bảo là mình đặt không phải trang thật, lúc đặt thì mình đặt ở web nt lại cho nó thì nó block mình luôn!((	Xem Xem	ĐÃ DUYỆT	XÓA

- Trang chủ: <https://antiscam-tgp.click/> [Trang chủ, Giới thiệu, Trang thông tin, Tìm kiếm, Tổ cáo và Báo cáo thống kê]



- ✓ Với "ANTI SCAM": có các chức năng:
  - **GIỚI THIỆU ANTISCAM-TGP.CLICK**
  - Sự ra đời ANTISCAM-TGP.CLICK.
  - Đưa ra: Ý tưởng (Phân tích, mục đích, lời khuyên)
  - Hệ thống website bao gồm 4 Mục: Giới thiệu, tố cáo lừa đảo, tìm kiếm, sử dụng ô tìm kiếm "Số điện thoại, STK ngân hàng" để tố cáo dữ liệu lừa đảo, "Trang thông tin" tìm hiểu nâng cao kiến thức về an ninh mạng, ...
  - Hoạt động dựa trên: nền tảng trình duyệt website.
  - **TRANG THÔNG TIN:** <https://antiscam-tgp.click/blog/>
  - **TÌM KIẾM HỒ SƠ LỪA ĐẢO:** Xem được các thông tin, những tài khoản lừa đảo trên không gian mạng.
  - **TỔ CÁO LỪA ĐẢO:** Tố cáo được những hồ sơ lừa đảo trên mạng xã hội, bao gồm: Họ và tên, số điện thoại, số tài khoản ngân hàng (kèm tên ngân hàng), ảnh chụp để xác minh bằng chứng, thông tin người tố cáo (gồm: họ và tên, thông tin liên lạc)
  - **BÁO CÁO THỐNG KÊ:** Tỷ lệ tương tác, số liệu hồ sơ tố cáo, số lần xem, thời lượng phiên hoạt động, số sự kiện.
- Trang thông tin: <https://antiscam-tgp.click/blog/> [Trang chủ, về tôi thông tin liên hệ, .....]



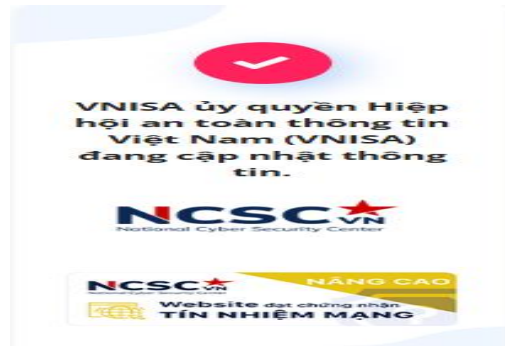
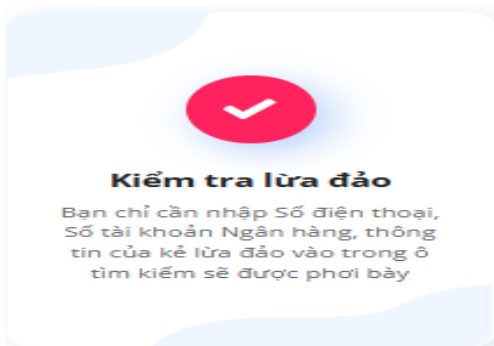
✓ **Với trang thông tin:** Trang có giao diện thân thiện người dùng, trực quan để sử dụng, bao gồm các bài viết về các kiến thức, kỹ năng, cung cấp nhiều thông tin về các hình thức lừa đảo, kiến thức – kỹ năng về bảo mật thông tin trên môi trường không gian mạng, giúp mọi người nâng cao kiến thức để bảo vệ thông tin cá nhân, từ đó giải quyết được phần nào về vấn nạn lừa đảo trên không gian mạng.

**Bao gồm các mục:** Trang chủ, thông tin liên hệ.

- Hoàn thành việc xây dựng cơ sở dữ liệu.

id	username	ly_do
56139	Lê Cường Quốc	lừa đảo tiền lấy lại fa
56140	Đeo Ngọc Thạch	Lừa đảo rất tinh vi tên thật Lê Cường Q
56141	Long Manh Hung	Lừa đảo, gửi tk mk x kêu...
56142	dang hoang gia bảo	scam web fake admin
56143	Nguyễn Vũ Luân	em có hỏi mua điện t co...
56144	dang hoang gia bảo	Lừa đảo, gửi tk mk x kêu...
56145	Hoàng Bảo Tiến	Lừa đảo mua bán cá
56146	Phạm Minh Trung	Đầu tiên bạn này là n ba...
56147	công ty TNHH Thương mại xuất nhập khẩu future p.	Nó tạo 1 trang bán h t...

- Xây dựng website cung cấp kiến thức thông tin để mọi người nâng cao kiến thức về an toàn thông tin trên không gian mạng.
- Được VNISA ủy quyền Hiệp hội an toàn thông tin Việt Nam (VNISA).
- Đạt chứng chỉ trang website an toàn National Cyber Security Centre (NCSC).



- Tổng quan về dữ liệu hiện hành gồm:

Website chức năng: 03

Website chính thức: 01

Website dự phòng: 02


Tên miền: 02

Website thông tin: 01

Website chức năng kiểm duyệt: 01

Dữ liệu: data 133.876 N (N=1.000) dữ liệu lừa đảo trên mạng xã hội & hàng trăm đơn

tổ cáo

Cảnh báo lừa đảo	
Họ và tên:	công ty TNHH thương mại xuất nhập khẩu future p.
Số điện thoại:	0126977798888
Số tài khoản	0126977798888
Ngân hàng	Mb Bank
Ảnh chụp bằng chứng	<p>o biến động số dư</p>  <p>Ngân</p>
Mô tả hình thức	Nó tạo 1 trang bán hàng y hệt trang chính hãng (tôi pedro). Rồi trang web cũng y hệt lúc đó mình không kiểm tra kĩ, mình đặt hàng ck trước đợi hoài không thấy m nt cho trang pedro. thật có tích xanh để hỏi thì được báo là mình đặt không phải trang thật. lúc đặt thì mình đặt ở web nt lại cho nó thì nó block mình luôn:((
Người tố cáo	
Họ và tên:	Anh Thư
Liên hệ:	03775*****

- Với các nền tảng trên được lập trình của bộ ba ngôn ngữ: Html, Javascript, Css.
- Máy chủ được sử dụng H2cloud.
- Sử dụng tên miền: antiscam-tgp
- Sử dụng Hosting: .click
- Sử dụng quản lý dữ liệu mã nguồn: cPanel, NodeJS
- Ngôn ngữ lập trình: Php.
- Server Information: ns1.h2cloud.vn, ns2.h2cloud.vn.
- Với địa chỉ IP: 103.77.240.59.
- Nguồn dữ liệu data: API bên thứ 3.

#### IV. Phạm vi nghiên cứu

Phạm vi nghiên cứu trong dự án xây dựng website phòng chống lừa đảo trên không gian mạng cần được xác định rõ ràng để đảm bảo tính khả thi và hiệu quả, bao gồm các yếu tố chủ yếu như loại hình lừa đảo, đối tượng người dùng, công nghệ và giải pháp kỹ thuật, cũng như các chính sách và hoạt động phòng chống. Dưới đây là các thành phần chính của phạm vi nghiên cứu:

##### 1. Phạm vi về loại hình lừa đảo trên không gian mạng

➤ **Lừa đảo qua email (Phishing):** Tập trung vào nghiên cứu các hình thức lừa đảo qua email, cách nhận diện các email giả mạo và cách bảo vệ thông tin cá nhân.

➤ **Lừa đảo qua mạng xã hội (Social Media Fraud):** Nghiên cứu các mảnh lừa đảo qua Facebook, Instagram, TikTok, Zalo, ... như lừa đảo qua tin nhắn, tài khoản giả, quảng cáo giả.

➤ **Lừa đảo qua điện thoại (Smishing, Vishing):** Tìm hiểu về các hình thức lừa đảo qua tin nhắn SMS, cuộc gọi điện thoại hoặc ứng dụng nhắn tin.

➤ **Lừa đảo tài chính (Investment Fraud):** Nghiên cứu các hình thức lừa đảo liên quan đến đầu tư tài chính như các dự án ảo, tiền điện tử giả mạo.

➤ **Lừa đảo qua website giả mạo (Fake Websites):** Nghiên cứu về các website giả mạo nhằm lừa đảo thông qua các chiêu thức như giả mạo thương hiệu, dịch vụ, và yêu cầu cung cấp thông tin cá nhân.

## 2. Phạm vi đối tượng người dùng

➤ **Người dùng Internet cá nhân:** sử dụng Internet cho mục đích cá nhân như mua sắm trực tuyến, học tập, giải trí, dễ bị lừa đảo qua nhiều hình thức khác nhau.

➤ **Doanh nghiệp và tổ chức:** Các tổ chức có thể là mục tiêu của các cuộc tấn công mạng nhằm xâm nhập hệ thống dữ liệu, chiếm đoạt thông tin tài chính hoặc tấn công website.

➤ **Người dùng dễ bị tổn thương:** Các nhóm như người cao tuổi, trẻ em hoặc người thiếu kinh nghiệm về an ninh mạng có nguy cơ cao bị lừa đảo.

## 3. Phạm vi nghiên cứu về công nghệ và giải pháp kỹ thuật

➤ **Phần mềm và công cụ bảo mật:** Nghiên cứu các phần mềm bảo mật, chống virus, tường lửa (firewalls), và các công nghệ nhận diện website giả mạo (anti-phishing).

➤ **Giải pháp phòng chống lừa đảo trực tuyến:** Nghiên cứu các giải pháp bảo mật như mã hóa thông tin, xác thực hai yếu tố (2FA), và các công nghệ bảo vệ khác.

## 4. Phạm vi nghiên cứu về giáo dục và nâng cao nhận thức

➤ **Tuyên truyền và giáo dục cộng đồng:** Tạo ra các chiến dịch tuyên truyền và các tài liệu hướng dẫn về cách nhận diện các hình thức lừa đảo phổ biến trên mạng.

➤ **Khóa học, hội thảo, video hướng dẫn:** Phát triển các khóa học trực tuyến, hội thảo hoặc video hướng dẫn về bảo mật, an toàn thông tin cho người dùng.

## 5. Phạm vi nghiên cứu về pháp lý và các chính sách

➤ **Luật pháp về bảo vệ người tiêu dùng:** Nghiên cứu các quy định pháp lý liên quan đến bảo vệ người tiêu dùng và xử lý các vụ lừa đảo trực tuyến.

➤ **Chính sách bảo mật dữ liệu:** Tìm hiểu các quy định về bảo mật thông tin cá nhân và các hành động pháp lý đối với hành vi lừa đảo qua mạng.

➤ **Xử lý vi phạm và hình thức xử lý:** Nghiên cứu về các biện pháp xử lý đối với những kẻ lừa đảo, bao gồm truy tố hình sự, xử phạt hành chính, và hỗ trợ người bị lừa đảo lấy lại tài sản.

## 6. Phạm vi nghiên cứu về các cơ chế hỗ trợ và giám sát

➤ **Hệ thống báo cáo và hỗ trợ người dùng:** Xây dựng hệ thống giúp người dùng báo cáo các vụ lừa đảo và nhận hỗ trợ từ cơ quan chức năng hoặc các tổ chức bảo vệ quyền lợi người tiêu dùng [<https://antiscam-tgp.click/pages/to-cao.php>].

➤ **Công cụ giám sát các hành vi lừa đảo:** Nghiên cứu về các công cụ giám sát và phát hiện các hành vi lừa đảo trực tuyến trong thời gian thực.

## 7. Phạm vi về khu vực nghiên cứu

➤ **Nghiên cứu toàn cầu với khu vực:** Dự án có thể tập trung vào một quốc gia, chẳng hạn như Việt Nam, hoặc nghiên cứu toàn cầu về các xu hướng và chiến lược phòng chống lừa đảo trên mạng.

➤ **Các đặc điểm địa phương:** Xem xét các xu hướng lừa đảo mạng tại các khu vực hoặc quốc gia cụ thể, như đặc thù tội phạm mạng tại các quốc gia đang phát triển.

**Tóm lại, phạm vi nghiên cứu của dự án website phòng chống lừa đảo trên không gian mạng-ANTI SCAM bao gồm các yếu tố chính như:**

- Các loại hình lừa đảo trên mạng.
- Đối tượng người dùng có thể bị ảnh hưởng.
- Các giải pháp kỹ thuật và công nghệ phòng chống.
- Giải pháp giáo dục và nâng cao nhận thức cộng đồng.
- Các vấn đề pháp lý và chính sách bảo vệ người dùng.
- Các cơ chế hỗ trợ, giám sát và báo cáo.

## V. Kế hoạch nghiên cứu và chuẩn bị thực hiện

### 1. Kế hoạch:

#### ❖ Mục tiêu nghiên cứu:

➤ **Tìm hiểu các hình thức lừa đảo trên không gian mạng:** Phân tích và nhận diện các loại lừa đảo phổ biến như phishing, smishing, vishing, các cuộc tấn công qua email, mạng xã hội và website giả mạo.

➤ **Nghiên cứu đối tượng người dùng dễ bị tổn thương:** Tìm hiểu về những đối tượng có nguy cơ cao bị lừa đảo và cách họ bị tấn công.

➤ **Đánh giá các giải pháp bảo mật:** Nghiên cứu các công nghệ bảo mật hiện tại và tìm giải pháp tối ưu để phòng chống lừa đảo.

➤ **Đề xuất các phương pháp nâng cao nhận thức cộng đồng:** Xây dựng chiến lược giáo dục và tuyên truyền hiệu quả để người dùng nâng cao khả năng nhận diện và phòng tránh lừa đảo.

➤ **Nghiên cứu các vấn đề pháp lý và chính sách bảo vệ người dùng:** Phân tích các luật và quy định bảo vệ người dùng trong việc phòng chống lừa đảo trên không gian mạng.

#### ❖ Phương pháp nghiên cứu:

##### ➤ *Nghiên cứu tài liệu thứ cấp:*

– **Tài liệu học thuật:** Đọc và phân tích các nghiên cứu, bài báo, tài liệu về các hình thức lừa đảo mạng và giải pháp bảo vệ người dùng.

– **Dữ liệu thống kê:** Thu thập dữ liệu từ các báo cáo, nghiên cứu thị trường, các tổ chức bảo mật và cơ quan pháp lý về các vụ lừa đảo trên mạng.

##### ➤ *Phương pháp nghiên cứu định tính:*

– **Phỏng vấn chuyên gia:** Phỏng vấn các chuyên gia trong lĩnh vực an ninh mạng (Huỳnh Ngọc Hải đạt giải ba cuộc thi an toàn thông tin, trường Học Viện Kỹ Thuật Mật



Mã KMA, Thanh Trì Hà Nội), nghiên cứu và cơ quan chức năng để thu thập thông tin về các xu hướng tội phạm mạng.

– **Khảo sát người dùng:** Tiến hành khảo sát người dùng mạng để hiểu về mức độ nhận thức và khả năng phòng tránh các hình thức lừa đảo trên mạng.

➤ **Phương pháp nghiên cứu định lượng:**

– **Phân tích dữ liệu:** Thu thập và phân tích dữ liệu về số lượng các vụ lừa đảo mạng, tỷ lệ người dùng bị ảnh hưởng và các đặc điểm liên quan.

– **Kiểm tra hiệu quả các giải pháp bảo mật:** Đánh giá hiệu quả của các công cụ bảo mật hiện có thông qua thử nghiệm và phân tích dữ liệu.

## 2. Chuẩn bị:

- Xác định mục tiêu nghiên cứu
- Nghiên cứu tài liệu và dữ liệu hiện có.
- Thiết lập quy trình nhiệm vụ từng khoảng thời gian trên Microsoft Project.
- Xây dựng kế hoạch dự án chi tiết.
- Xác định đối tượng người dùng và khảo sát ban đầu.
- Xây dựng mô hình Website và các tính năng chính.
- Chuẩn bị các tài nguyên hỗ trợ.
- Nguồn kinh phí và tài trợ.

Giai đoạn chuẩn bị là bước đầu tiên trong dự án **Website phòng chống lừa đảo trên không gian mạng-ANTI SCAM**, bao gồm các công việc như xác định mục tiêu nghiên cứu, nghiên cứu tài liệu hiện có, xây dựng đội ngũ nghiên cứu, lập kế hoạch chi tiết và chuẩn bị tài nguyên. Mục đích của giai đoạn này là tạo ra nền tảng vững chắc cho việc triển khai các bước nghiên cứu và phát triển trong các giai đoạn tiếp theo của dự án.

## 3. Thực hiện:

### ❖ Các giai đoạn:

- **Giai đoạn 1:** Chuẩn bị và nghiên cứu cơ sở.
- **Giai đoạn 2:** Thu thập dữ liệu và nghiên cứu thực tiễn.
- **Giai đoạn 3:** Phát triển giải pháp và công cụ phòng chống.
- **Giai đoạn 4:** Kiểm tra và đánh giá.
- **Giai đoạn 5:** Phân tích và báo cáo kết quả.

### ❖ Tổng thời gian nghiên cứu: 11 tháng

- **Giai đoạn 1:** 1 tháng
- **Giai đoạn 2:** 3 tháng
- **Giai đoạn 3:** 3 tháng
- **Giai đoạn 4:** 2 tháng
- **Giai đoạn 5:** 2 tháng



## VI. Thành tựu số liệu nghiên cứu

### ❖ Số liệu đánh giá mức độ nhận thức của người dùng về các mối nguy hiểm và các hành vi phòng tránh lừa đảo trên mạng:

- **Tỷ lệ người dùng nhận diện đúng các dấu hiệu của lừa đảo giảm 54%:** Bao gồm việc phát hiện email giả mạo, các website không an toàn, hoặc các quảng cáo lừa đảo trên mạng xã hội.
- **Tỷ lệ người dùng sử dụng các biện pháp bảo mật đạt 78%:** Như xác thực hai yếu tố (2FA), phần mềm chống virus và cài đặt tường lửa.
- **Tỷ lệ người dùng không sử dụng biện pháp bảo mật 22%:** Thông qua khảo sát để hiểu lý do tại sao một số người không sử dụng các công cụ bảo mật.

### ❖ Toàn thể số liệu “DỰ ÁN PHÒNG CHỐNG LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG - ANTI SCAM”

- Hoàn thành mô hình hoạt động thực tế và luân chuyển dữ liệu giữa các trang web. Kết hợp hiển thị kết nối các trang web cho phép người dùng tối ưu hóa việc sử dụng.
- Thống kê số liệu hoạt động tính tới thời điểm 15/7/2025:
  - ✓ Tổng số tỷ lệ tương tác: **95,4%**.
  - ✓ Tổng số hồ sơ tố cáo: **133.876 N** (với N=1.000).
  - ✓ Tổng số lần xem: **132 N**.
  - ✓ Tổng số sự kiện: **121 N**.
  - ✓ Thời gian tương tác trung bình: **42 phút**.
  - ✓ Tổng số thời gian người xem tương tác hoạt động trên nền tảng: **18.543** giờ

## VII. Kết luận

Như vậy, có thể thấy cùng với sự phát triển của công nghệ thông tin cũng như xu thế thay đổi văn hóa làm việc và học tập, thì các chiến dịch tấn công lừa đảo cũng ngày càng gia tăng và tinh vi hơn và thường nhắm đến các tổ chức, cá nhân tài chính nơi mà có nhiều thông tin dữ liệu cũng như tài sản có giá trị. Bên cạnh đó những nhóm đối tượng dễ bị tổn thương: như nhóm người cao tuổi, trẻ em hoặc người thiếu kinh nghiệm về an ninh mạng có nguy cơ cao bị lừa đảo.

Lừa đảo trên không gian mạng đang là một vấn đề rất phức tạp, đặc biệt nguy hiểm đối với toàn cầu nói chung và những người chưa có nhiều kinh nghiệm đối phó của một quốc gia nói riêng. Chính vì vậy, bằng cách nâng cao nhận thức, cập nhật thông tin và thực hiện các biện pháp bảo vệ thông tin cá nhân và giúp đỡ mọi người phòng tránh các rủi ro tiềm ẩn trên không gian số. Đó cũng là lý do tôi đưa ra kế hoạch và nghiên cứu dự án “**Phòng chống lừa đảo trên không gian mạng-ANTISCAM**”

1. Website <https://antiscam-tgp.click/> giúp mọi người có thể dễ dàng kiểm tra được thông tin về: số điện thoại, số tài khoản ngân hàng, địa chỉ trang web nghi vấn có dấu hiệu lừa đảo để tố cáo kẻ lừa đảo một cách dễ dàng

2. Trang thông tin của Website <https://antiscam-tgp.click/blog/> giúp người dùng đọc được những thông tin hữu ích, tiện lợi, về các hình thức lừa đảo, diệt virus, các đề phòng lừa đảo,...

Trang thống kê kết quả nghiên cứu: <https://antiscam-tgp.click/pages/baocao.php#>

### Thống kê tổng quan



### VIII. Nguồn tham khảo

1. Wikipedia, youtube, ...
2. Kho dữ liệu hình ảnh video, Adobe Photoshop, Adobe Illustrator, Canva ...
3. Nguồn dữ liệu thu thập từ Internet.
4. Bộ thông tin và truyền thông, báo Ấp Bắc
5. Chuyên gia công nghệ Ngô Minh Hiếu (Hiếu PC ).
6. Ban chuyên đề Công an TPHCM.
7. Các nguồn tài liệu khác, .....