SỔ TAY CÔNG NGHỆ SỐ CỘNG ĐỒNG TỈNH LAI CHÂU

BỘ QUY TẮC
ỨNG XỬ TRÊN MẠNG XÃ HỘI

MỤC ĐÍCH CỦA BỘ QUY TẮC ỨNG XỬ TRÊN MẠNG XÃ HỘI

- Tạo điều kiện phát triển lành mạnh mạng xã hội tại Việt Nam
- Bảo đảm quyền tự do cá nhân, quyền tự do kinh doanh, không phân biệt đối xử nhà cung cấp dịch vụ trong và ngoài nước
- Phù hợp với chuẩn mực, thông lệ và các điều ước quốc tế mà Việt Nam đã tham gia.
- Xây dựng chuẩn mực đạo đức về hành vi, ứng xử trên mạng xã hội
- Giáo dục ý thức, tạo thói quen tích cực trong các hành vi ứng xử của người dùng trên mạng xã hội
- Góp phần xây dựng môi trường mạng an toàn, lành mạnh tại Việt Nam.

ĐỐI TƯỢNG ÁP DỤNG BỘ QUY TẮC ỨNG XỬ TRÊN KHÔNG GIAN MẠNG

Cơ quan nhà nước, cán bộ, công chức, viên chức, người lao động trong cơ quan nhà nước sử dụng mạng xã hội.

Tổ chức, cá nhân khác sử dụng mạng xã hội.

Nhà cung cấp dịch vụ mạng xã hội tại Việt Nam

QUY TẮC ỨNG XỬ CHUNG

Quy tắc Tôn trọng, tuân thủ pháp luật: Tuân thủ pháp luật Việt Nam, tôn trọng quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Quy tắc Lành mạnh: Hành vi, ứng xử trên mạng xã hội phù hợp với các giá trị đạo đức, văn hóa, truyền thống tốt đẹp của dân tộc Việt Nam.

Áp dụng cho tất cả các nhóm đối tượng

Quy tắc Trách nhiệm: Chịu trách nhiệm về các hành vi, ứng xử trên mạng xã hội; phối hợp với các cơ quan chức năng để xử lý hành vi, nội dung thông tin vi phạm pháp luật.

Quy tắc An toàn, bảo mật thông tin: Tuân thủ các quy định và hướng dẫn về bảo vệ an toàn và bảo mật thông tin.

QUY TẮC ỨNG XỬ CHO TỔ CHỨC, CÁ NHÂN KHÁC

1. Tìm hiểu và tuân thủ các điều khoản hướng dẫn sử dụng của nhà cung cấp dịch vụ mạng xã hội trước khi đăng ký, tham gia mạng xã hội.

3. Thực hiện biện pháp tự quản lý, bảo mật tài khoản mạng xã hội và nhanh chóng thông báo tới các cơ quan chức năng, nhà cung cấp dịch vụ khi tài khoản tổ chức, cá nhân bị mất quyền kiểm soát, bị giả mạo, lợi dụng và sử dụng vào mục đích không lành mạnh, ảnh hưởng đến an ninh quốc gia và trật tự an toàn xã hội, ảnh hưởng đến quyền và lợi ích hợp pháp của tổ chức, cá nhân.

2. Nên sử dụng họ, tên thật cá nhân, tên hiệu thật của tổ chức, cơ quan và đăng ký với nhà cung cấp dịch vụ để xác thực tên hiệu, địa chỉ trang mạng, đầu mối liên lạc khi tham gia, sử dụng mạng xã hội.

4. Chia sẻ những thông tin có nguồn chính thống, đáng tin cậy.

QUY TẮC ỨNG XỬ CHO TỔ CHỨC, CÁ NHÂN KHÁC

5. Các hành vi, ứng xử phù hợp với những giá trị đạo đức, văn hóa, truyền thống của dân tộc Việt Nam; không sử dụng từ ngữ gây thù hận, kích động bạo lực, phân biệt vùng miền, giới tính, tôn giáo.

6. Không đăng tải những nội dung vi phạm pháp luật, các thông tin xúc phạm danh dự, nhân phẩm ảnh hưởng đến quyền và lợi ích hợp pháp của các tổ chức, cá nhân khác; sử dụng ngôn ngữ phản cảm, vi phạm thuần phong mỹ tục; tung tin giả, tin sai sự thật; quảng cáo, kinh doanh dịch vụ trái phép... gây bức xúc trong dư luận xã hội, ảnh hưởng đến trật tự an toàn xã hội.

7. Khuyến khích sử dụng mạng xã hội để tuyên truyền, quảng bá về đất nước - con người, văn hóa tốt đẹp của Việt Nam, chia sẻ thông tin tích cực, những tấm gương người tốt, việc tốt.

8. Vận động người thân trong gia đình, bạn bè, những người xung quanh tham gia giáo dục, bảo vệ trẻ em, trẻ vị thành niên sử dụng mạng xã hội một cách an toàn, lành mạnh.

QUY TẮC ỨNG XỬ CHO CÁN BỘ, CÔNG CHỨC, VIÊN CHỨC VÀ NGƯỜI LAO ĐỘNG TRONG CƠ QUAN NHÀ NƯỚC

1. Cán bộ, công chức, viên chức và người lao động trong cơ quan nhà nước thực hiện nội dung Quy tắc ứng xử cho tổ chức, cá nhân khác

2. Thực hiện nội quy của cơ quan, tổ chức về việc cung cấp thông tin lên mạng xã hội.

3. Thông báo tới cơ quan chủ quản để kịp thời có hướng xử lý, trả lời, giải quyết khi có những ý kiến, thông tin trái chiều, thông tin vi phạm pháp luật có liên quan đến chức năng, nhiệm vụ, quyền hạn, lĩnh vực quản lý của cán bộ, công chức, viên chức và người lao động."

QUY TẮC ỨNG XỬ CHO CÁC CƠ QUAN NHÀ NƯỚC

1. Thực hiện nội dung quy định Quy tắc ứng xử cho tổ chức, cá nhân khác.

2. Có trách nhiệm quản lý, bảo mật tài khoản mạng xã hội và nhanh chóng thông báo tới nhà cung cấp dịch vụ khi tài khoản của cơ quan, tổ chức bị mất quyền kiểm soát hoặc bị giả mạo.

3. Cung cấp thông tin trên mạng xã hội đồng bộ, thống nhất với thông tin đã được cung cấp trên các phương tiện truyền thông chính thống khác.

4. Nên có phản hồi những ý kiến trên mạng xã hội về vấn đề liên quan đến chức năng, nhiệm vụ và quyền hạn của cơ quan, tổ chức mình.

QUY TẮC ỨNG XỬ CHO CÁC NHÀ CUNG CẤP DỊCH VỤ MẠNG XÃ HỘI

1. Công bố rõ ràng các điều khoản sử dụng dịch vụ, bao gồm tất cả các quyền và nghĩa vụ của nhà cung cấp dịch vụ và người sử dụng.

2. Ban hành và công khai các biện pháp phát hiện, thông báo và phối hợp với các cơ quan chức năng để xử lý, ngăn chặn và loại bỏ các nội dung thông tin vi phạm bản quyền, vi phạm pháp luật.

3. Khi nhận được thông báo yêu cầu loại bỏ các thông tin vi phạm bản quyền, vi phạm pháp luật từ cơ quan chức năng có thẩm quyền, nhà cung cấp dịch vụ mạng xã hội phối hợp với tổ chức, cá nhân sử dụng mạng xã hội để xử lý theo các quy định của pháp luật Việt Nam.

4. Hướng dẫn người sử dụng mạng xã hội, hỗ trợ và bảo vệ quyền, lợi ích hợp pháp của "người yếu thế" trong xã hội (người nghèo, người dân tộc thiểu số, trẻ em, trẻ vị thành niên, người khuyết tật...) sử dụng mạng xã hội an toàn, lành mạnh nhằm tránh bị khai thác, lạm dụng, bạo lực về tinh thần trên mạng xã hội; có biện pháp để bảo đảm sự an toàn và phát triển lành mạnh của trẻ em, trẻ vị thành niên trên mạng xã hội theo quy định của pháp luật Việt Nam.

5. Tôn trọng quyền được bảo vệ thông tin của người sử dụng, không thu thập thông tin cá nhân và cung cấp thông tin của người sử dụng dịch vụ cho bên thứ ba khi chưa được sự cho phép của chủ thể thông tin.

CẨM NANG
NHẬN DIỆN VÀ PHÒNG CHỐNG LỪA ĐẢO TRỰC TUYẾN

LỪA ĐẢO
"COMBO DU LỊCH GIÁ RẺ"

1 RẺ 30-50% SO VỚI GIÁ CHUNG

- Cảnh giác khi nhận được lời mời chào mua gói du lịch với mức giá quá rẻ (rẻ hơn 30-50% so với giá chung của thị trường).
- Đặc biệt thận trọng khi đơn vị du lịch yêu cầu chuyển tiền đặt cọc để giữ chỗ, nếu có thể nên thực hiện giao dịch thanh toán trực tiếp.

2 HOÀN TRẢ 100% TIỀN LÀM VISA

- Đăng bài viết quảng cáo dịch vụ làm visa (thị thực) du lịch nước ngoài, cam kết tỷ lệ thành công cao, hoàn trả 100% số tiền nếu không xin được visa.
- Sau khi nạn nhân chuyển khoản thanh toán chi phí hoặc một phần chi phí, đối tượng lừa đảo sẽ để nạn nhân tự khai thông tin tờ khai, hoàn thiện hồ sơ... Sau đó lấy lý do nạn nhân khai thông tin bị thiếu và không trả lại tiền.

3 GIẢ MẠO FANPAGE/WEBSITE

- Làm giả website/fanpage của công ty du lịch uy tín, làm giả ảnh chụp biên lai, hóa đơn thanh toán và đề nghị nạn nhân chuyển khoản thanh toán chi phí tour du lịch.
- Thông thường tên các website giả sẽ gần giống với tên các website thật nhưng sẽ có thêm hoặc thiếu một số ký tự. Tên miền giả thường sử dụng những đuôi lạ như .cc, .xyz, .tk...

4 BỊ MẮC KẸT TẠI NƯỚC NGOÀI

- Làm giả/chiếm đoạt tài khoản của người dùng mạng xã hội, sử dụng công nghệ Deepfake (tạo ra các đoạn video với hình ảnh, khuôn mặt, giọng nói nhân vật giống như hình ảnh của người muốn giả mạo) để lừa đảo.
- Liên lạc với người thân trong danh sách bạn bè cho biết đang bị mắc kẹt khi du lịch tại nước ngoài và cần một khoản tiền ngay lập tức.

5 MẠO DANH ĐẠI LÝ VÉ MÁY BAY

- Mạo danh đại lý bán vé máy bay, làm giả website, trang mạng xã hội, đường dẫn với gia diện gần giống với kênh chính thức, sau đó quảng cáo với các mức giá rất hấp dẫn so với mặt bằng chung để thu hút khách hàng.
- Người dân nên chọn các trang mạng xã hội có dấu tích xanh (tài khoản đã đăng ký) hoặc chọn các trang mạng xã hội có uy tín mà mình biết rõ thông tin của người bán.


DEEPFAKE
THỜI GIAN gọi thường rất ngắn chỉ vài giây.
01
KHUÔN MẶT người gọi thiếu tính cảm xúc và khá "trơ" khi nói hoặc tư thế trông lúng túng, không tự nhiên hoặc hướng đầu và cơ thể của họ trong video không nhất quán với nhau...
02
MÀU DA của nhân vật trong video bất thường, ánh sáng kỳ lạ và bóng đổ không đúng vị trí, video trông rất giả tạo và không tự nhiên.
03
ÂM THANH sẽ không đồng nhất với hình ảnh, có nhiều tiếng ồn bị lạc vào clip hoặc clip không có âm thanh.
04
NGẮT MÁY GIỮA CHỪNG với lý do mất sóng, sóng yếu...
05

DẤU HIỆU NHẬN BIẾT

- Người gọi xưng là người của Bộ Thông tin & Truyền thông hoặc là Cục Viễn thông.
- Dọa khóa sim trong vòng 2 tiếng với các lý do như "chưa nộp phạt", "thuê bao sai thông tin",...
- Bắt khai báo thông tin cá nhân hoặc thực hiện các cú pháp sang tên đổi chủ số điện thoại, chuyển hướng cuộc gọi...

NGUY CƠ GẶP PHẢI

- Khi đã chiếm được quyền nhận cuộc gọi, các đối tượng lừa đảo sẽ đăng nhập ứng dụng ví điện tử, tài khoản mạng xã hội... của nạn nhân và khai báo quên mật khẩu đăng nhập, chọn tính năng nhận cuộc gọi thông báo mã OTP.
- Từ đó, đối tượng lừa đảo dễ dàng chiếm đoạt tài khoản mạng xã hội, kiểm soát chiếm đoạt tiền trong ví, tài khoản ngân hàng liên kết với ví điện tử.

CẦN LÀM GÌ

- Chủ động kiểm tra thông tin đã chuẩn hóa hay chưa thông qua các công cụ, hướng dẫn từ nhà mạng
- Không thực hiện theo các yêu cầu khi nghe cuộc gọi từ số điện thoại lạ.
- Đối với các thuê bao đã bị khóa hai chiều, phải đến trực tiếp các điểm giao dịch của các nhà mạng để thực hiện chuẩn hóa và mở khóa liên lạc lại.

CẢNH BÁO GIẢ MẠO BIÊN LAI CHUYỂN TIỀN

DẤU HIỆU

- Mua hàng số lượng lớn.
- Chụp màn hình "Giao dịch thành công" nhưng chưa nhận được tiền trong tài khoản.

CẢNH BÁO

Hoạt động cung cấp và mua bán biên lai xác nhận chuyển khoản giả đang được diễn ra một cách công khai, lộ liễu trên mạng xã hội. Hình ảnh bill chuyển khoản tinh vi, giống y như thật.

NÊN LÀM

Không giao hàng hóa khi chưa nhận được tiền trong tài khoản ngân hàng, kể cả khi nhận được hình ảnh đã "chuyển khoản thành công".

GIẢ DANH GIÁO VIÊN/NHÂN VIÊN Y TẾ

Báo người thân đang cấp cứu

DẤU HIỆU	BIỆN PHÁP
Tự xưng là giáo viên/nhân viên y tế, gọi điện cho phụ huynh, học sinh thông báo rằng con/ người thân đang cấp cứu trong tình trạng nguy kịch, thúc giục cha mẹ chuyển tiền.	Hạn chế, không chia sẻ, cung cấp thông tin cá nhân lên mạng xã hội hoặc cho bất kỳ ai không quen biết; tuyệt đối không truy cập các đường link lạ hoặc không rõ nguồn gốc.
Đánh vào tâm lý, tình cảm của nạn nhân, hình thành trạng thái bất an, lo sợ và hoảng loạn; trình bày không rõ ràng về tình trạng, sử dụng những ngôn từ tiêu cực.	Khi nhận các cuộc điện thoại, tin nhắn bất thường, người dân cần bình tĩnh xác minh thông tin, xem xét cẩn thận, không vội vàng trả lời hay thực hiện theo nội dung mà đối tượng đưa ra.
Một số đối tượng còn thuộc lòng thông tin về trường, lớp học của con, tên giáo viên chủ nhiệm, thầy cô, hiệu trưởng khiến phụ huynh nhất thời tin tưởng.	Các tổ chức, cá nhân có thể truy cập vào cổng thông tin khonggianmang.vn để tra cứu hoặc phản ánh tới cơ quan chức năng.
Cách xưng hô khác thường ngày, không thể cung cấp thông tin cá nhân của mình một cách rõ ràng, thời gian gọi điện vào giờ nghỉ trưa, giữa đêm hay giờ tan tầm.	Trường hợp nghi vấn đối tượng giả mạo, chiếm đoạt tài sản, cần báo ngay cho cơ quan công an gần nhất để được hỗ trợ, xử lý kịp thời.

LỪA ĐẢO
TUYỂN NGƯỜI MẪU NHÍ

DẤU HIỆU NHẬN BIẾT

Thủ đoạn của các đối tượng thường là:

Thông qua mạng xã hội: Facebook, Zalo, Telegram..., các đối tượng lừa đảo sẽ kết bạn với phụ huynh và mời tham gia ứng tuyển người mẫu nhí cho hãng thời trang.

Sau khi nạn nhân "cắn câu", các đối tượng lừa đảo sẽ đưa nạn nhân vào một group chat để mời tham gia thử thách.

Thử thách cho các phụ huynh khi muốn con mình tham gia vào ứng tuyển là chuyển khoản để mua sản phẩm hàng hiệu, sau đó chụp ảnh và quảng bá sản phẩm.

Đối tượng lừa đảo sẽ trả hoa hồng và tiến làm nhiệm vụ để "kích thích" phụ huynh tham gia, nhưng khi số tiền chuyển vào tăng cao, chúng xóa tung tích để chiếm đoạt tài sản.

BIỆN PHÁP PHÒNG TRÁNH

Để phòng tránh lừa đảo và những hậu quả đáng tiếc xảy ra, người dân cần lưu ý:

Không cung cấp những thông tin cá nhân cho người lạ, người không quen biết trên không gian mạng; không kết bạn, không vào các nhóm Zalo, Facebook, Telegram... không quen

Đặc biệt cẩn trọng đối với các chương trình tuyển mẫu nhí trên không gian mạng; đặc biệt không làm việc với nhà tuyển dụng nào yêu cầu chuyển tiền, nộp tiền trước.

Nên kiểm tra tác giả, đọc kỹ nội dung để xác định thông tin thật hay giả; tin tức giả thường sẽ bị lỗi chính tả hoặc có bố cục lộn xộn, thông tin liên hệ không rõ ràng.

Chỉ thực hiện giao dịch chuyển tiền khi xác định chắc chắn định danh của người mình trao đổi và tuyệt đối không click vào những đường link lạ.

GIẢ MẠO CÔNG TY TÀI CHÍNH, NGÂN HÀNG THU THẬP THÔNG TIN

DẤU HIỆU NHẬN BIẾT

Đánh vào tâm lý của những người đang cần tiền kinh doanh, tiêu xài, muốn được vay với số tiền lớn nhưng lại gặp khó.

Các đối tượng lừa đảo tạo lập hàng nghìn tài khoản Facebook với các nguồn thông tin giả, tham gia vào các hội nhóm, diễn đàn, đăng bài quảng cáo cho vay tín chấp.

Khi người vay chuyển tiền vào số tài khoản của các đối tượng cung cấp, các đối tượng sẽ lập tức chiếm đoạt và ngắt liên lạc.

CÁCH PHÒNG TRÁNH

Chủ động nâng cao ý thức cảnh giác trước các thủ đoạn lừa đảo chiếm đoạt tài sản. Khi có nhu cầu vay tiền, cần liên hệ trực tiếp với các tổ chức tín dụng, chi nhánh ngân hàng để được tư vấn, hướng dẫn.

Cảnh giác, tìm hiểu kỹ, xác thực chính xác công ty tài chính, tư vấn viên trước khi tiến hành các thủ tục vay tiền; nên tư vấn thêm ý kiến của người thân có nhiều kinh nghiệm trước khi làm các thủ tục.

Không cung cấp bất kỳ thông tin cá nhân (Căn cước công dân, địa chỉ, hình ảnh nhận diện khuôn mặt,...) khi chưa xác định chính xác website, ứng dụng và danh tính tư vấn viên.

Nhanh chóng trình báo cơ quan Công an nơi gần nhất khi phát triển thủ đoạn mạo danh, lừa đảo chiếm đoạt tài sản hoặc bị mạo danh, lừa đảo chiếm đoạt tài sản.

CÀI CẮM ỨNG DỤNG LINK QUẢNG CÁO TÍN DỤNG ĐEN CỜ BẠC CÁ ĐỘ

DẤU HIỆU

- Thường được quảng cáo rộng rãi trên các trang web với những tiêu đề thu hút hoặc nhắn tin qua số điện thoại kèm theo đường link đến ứng dụng...
- Thường mạo danh hoặc giả mạo là một công ty để gây dựng lòng tin ban đầu đối với nạn nhân.
- Khi người dùng đồng ý cấp quyền truy cập danh bạ, hình ảnh thì các ứng dụng này cũng sẽ sao lưu được các thông tin số điện thoại có trong danh bạ cũng như các hình ảnh được lưu trong điện thoại.

BIỆN PHÁP

- Nếu cần vay tiền, bạn nên tìm đến các tổ chức cho vay uy tín như ngân hàng hoặc các công ty tài chính hợp pháp.
- Tuyệt đối không cung cấp bất kỳ thông tin cá nhân, tài khoản ngân hàng trên các trang web và ứng dụng không tin cậy.
- Xem xét cẩn thận các quyền mà ứng dụng yêu cầu cũng như đọc kỹ các điều khoản, chính sách của ứng dụng này.

GIẢ MẠO

TRANG THÔNG TIN ĐIỆN TỬ CƠ QUAN, DOANH NGHIỆP

BIỆN PHÁP

Sử dụng phần mềm bảo mật 01

Cài đặt và duy trì phần mềm diệt virus, phần mềm chống độc, tường lửa và các công cụ bảo mật khác trên thiết bị và cập nhật thường xuyên.

Đào tạo và nhận biết 02

Hãy tự trang bị kiến thức về các phương pháp tấn công và các dấu hiệu nhận biết trang web lừa đảo qua tinnhiemmang.vn hoặc ncsc.gov.vn, theo dõi và cập nhật tại khonggianmang.vn

Kiểm tra đánh giá và phản hồi 03

Trước khi thực hiện giao dịch hoặc cung cấp thông tin cá nhân, hãy kiểm tra các đánh giá và phản hồi từ người dùng khác về trang web đó.

Phương pháp xác thực 04

Nếu có sẵn, hãy sử dụng các phương pháp xác thực bổ sung như xác thực hai yếu tố hoặc sử dụng mã OTP (One - Time Password).

Thông báo đột xuất 05

Cẩn thận với các thông báo đột xuất yêu cầu cập nhật thông tin cá nhân hoặc yêu cầu thay đổi mật khẩu.

BIỆN PHÁP

Kiểm tra địa chỉ URL 06

Hãy chắc chắn rằng địa chỉ URL chính xác và tương ứng với trang web mà bạn mong muốn.

Sử dụng trình duyệt an toàn 07

Các trình duyệt như Google Chrome, Mozilla Firefox và Safari thường có các cơ chế bảo mật tích hợp giúp ngăn chặn truy cập vào trang web độc hại.

Kiểm tra kết nối an toàn 08

Hãy đảm bảo rằng kết nối là an toàn bằng cách kiểm tra xem trang web có chứng chỉ SSL hợp lệ hay không.

Cẩn thận với email và liên kết 09

Tránh nhấp vào liên kết trong email không xác định hoặc không mong muốn. Kiểm tra nguồn gốc của email và đảm bảo rằng nó là đáng tin cậy trước khi tiếp tục.

Thông tin cá nhân 10

Chỉ cung cấp thông tin cá nhân nhạy cảm trên các trang web đáng tin cậy và an toàn.

GIẢ MẠO

SMS BRANDNAME

THỦ ĐOẠN GIẢ MẠO

Thiết lập trạm thu phát sóng viễn thông giả mạo, phát tán tin nhắn mạo danh thương hiệu của các tổ chức tài chính, ngân hàng, nhằm mục đích lừa đảo chiếm đoạt tiền của người dân.

BIỆN PHÁP PHÒNG TRÁNH

Đọc kỹ nội dung tin nhắn, kiểm tra các lỗi chính tả, xem xét một cách tỉnh táo, cẩn thận, không vội và trả lời hay thực hiện theo nội dung trong tin nhắn.

Khi nhận được các tin nhắn có dấu hiệu bất thường phải liên lạc ngay với đơn vị chủ quản của brandname thông qua hotline.

Tuyệt đối không truy cập các đường link, liên kết trong tin nhắn lạ hoặc không rõ nguồn gốc.

Lưu lại các bằng chứng, thực hiện phản ánh tới Doanh nghiệp viễn thông quản lý thuê bao để yêu cầu xử lý và cung cấp các bằng chứng đã có tới các cơ quan chức năng của Bộ Công an nơi gần nhất để nghị xử lý.

Không cung cấp tên, mật khẩu đăng nhập ngân hàng trực tuyến, mã xác thực OTP, số thẻ ngân hàng qua điện thoại, email, mạng xã hội và các trang web.

Theo dõi và cập nhật các thông tin, tình huống, dấu hiệu về lừa đảo trực tuyến tại khonggianmang.vn và gửi phản ánh về địa chỉ http://canhbao.khonggianmang.gov.vn

DẤU HIỆU NHẬN BIẾT

LỜI HỨA QUÁ CAO
Sàn đầu tư lừa đảo thường hứa lợi nhuận vượt trội, không thể tin được và quá cao so với thị trường thực

THIẾU THÔNG TIN MINH BẠCH
Sàn không cung cấp đầy đủ thông tin về công ty, giấy phép hoạt động, lịch sử giao dịch và nhân sự quản lý.

YÊU CẦU CHUYỂN TIỀN TRƯỚC
Sàn yêu cầu người tham gia chuyển khoản trước khi bắt đầu giao dịch, thường là dưới hình thức phí đăng ký, phí tham gia hoặc tiền ký quỹ.

THIẾU SỰ KIỂM SOÁT VÀ GIÁM SÁT
Sàn không có sự kiểm soát từ các cơ quan quản lý hoặc không được cấp phép hoạt động đúng quy định.

BIỆN PHÁP PHÒNG TRÁNH

TÌM HIỂU VỀ HỆ THỐNG BẢO MẬT

Đối với các sàn giao dịch và công ty trực tuyến, hãy tìm hiểu về hệ thống bảo mật và cơ chế bảo vệ thông tin cá nhân và tài sản của người dùng.

ĐÁNH GIÁ TỪ NGƯỜI DÙNG

Tìm hiểu và đánh giá từ người dùng khác về trải nghiệm của họ với sàn giao dịch hoặc công ty mà bạn quan tâm.

CẢNH GIÁC VỚI MỨC PHÍ VÀ CHI PHÍ

Hãy cẩn trọng với các khoản phí và chi phí không rõ ràng hoặc quá cao so với thị trường thông thường.

THẬN TRỌNG VỚI CÁC LỜI MỜI GIỚI THIỆU

Hãy cẩn trọng khi người khác đề nghị hoặc giới thiệu các hoạt động đầu tư mà bạn không biết gì về.

TÌM KIẾM TƯ VẤN CHUYÊN GIA

Nếu bạn không chắc chắn về một sàn giao dịch hoặc công ty, hãy tìm sự tư vấn từ chuyên gia tài chính hoặc luật sư để đảm bảo rằng bạn đưa ra quyết định thông minh và an toàn.

LỪA ĐẢO

TUYỂN DỤNG CỘNG TÁC VIÊN ONLINE

YÊU CẦU TẠM ỨNG TIỀN

Nếu bạn được yêu cầu nộp một khoản tiền tạm ứng trước khi bắt đầu công việc, hãy cảnh giác.

YÊU CẦU THÔNG TIN TÀI KHOẢN CÁ NHÂN

Lừa đảo có thể yêu cầu bạn cung cấp thông tin tài khoản cá nhân, số thẻ tín dụng, thông tin ngân hàng để thực hiện thanh toán hoặc tạo tài khoản.

TRANG THANH TOÁN KHÔNG AN TOÀN

Kiểm tra xem trang thanh toán đơn hàng có đủ các biểu tượng bảo mật như khóa SSL hay "https://" trước URL không.

QUẢNG CÁO CÔNG VIỆC QUÁ HẤP DẪN VÀ DỄ DÀNG

Lừa đảo thường hứa hẹn công việc có thu nhập cao và dễ dàng mà không yêu cầu kỹ năng hay kinh nghiệm đặc biệt.

THIẾU THÔNG TIN HOẶC KHÔNG CÓ THÔNG TIN LIÊN HỆ

Nếu không có thông tin rõ ràng hoặc không có thông tin liên hệ, đó có thể là dấu hiệu của một hoạt động lừa đảo.

THIẾU HỢP ĐỒNG HOẶC THỎA THUẬN RÕ RÀNG

Khi tham gia vào một chương trình tuyển cộng tác viên, hãy yêu cầu và đọc kỹ hợp đồng hoặc thỏa thuận liên quan.

KIỂM TRA ĐÁNH GIÁ VÀ PHẢN HỒI TIÊU CỰC

Nếu có nhiều phản hồi tiêu cực hoặc đánh giá không tốt, hãy cân nhắc trước khi tham gia.

LỪA ĐẢO

ĐÁNH CẮP TÀI KHOẢN MẠNG XÃ HỘI

DẤU HIỆU NHẬN BIẾT

1. Tin nhắn, email hoặc đường link đáng ngờ; sự thay đổi đột ngột trong ngôn ngữ hoặc phong cách viết.
2. Yêu cầu cung cấp thông tin cá nhân hay thông tin đăng nhập hoặc xác minh thông tin.
3. Hãy báo cáo và cảnh báo cho người bị ảnh hưởng và nền tảng mạng xã hội hoặc dịch vụ để họ thực hiện biện pháp cần thiết.

BIỆN PHÁP PHÒNG TRÁNH

1. Thay đổi mật khẩu ngay lập tức của tài khoản mạng xã hội và sử dụng một mật khẩu mạnh, bao gồm cả chữ hoa, chữ thường, số và ký tự đặc biệt.
2. Báo cáo sự cố thông qua mạng xã hội hoặc các liên hệ khác như điện thoại, email.
3. Thông báo cho bạn bè và người thân về tình huống và cảnh báo họ không nên tin tưởng hoặc phản hồi vào những tin nhắn lừa đảo.


1
Người bán/ Kênh bán
Hãy kiểm tra thông tin về người bán/ kênh bán, bao gồm địa chỉ, số điện thoại,... Nếu người bán áp đặt áp lực mua hàng ngay lập tức với lý do rằng số lượng có hạn hoặc chỉ giảm giá trong xx giờ thì nên cảnh giác.
2
Thông tin sản phẩm
Đọc kỹ thông tin chi tiết về sản phẩm, bao gồm hình ảnh, mô tả, thông số kỹ thuật và chính sách bảo hành. Nếu có bất kỳ thông tin thiếu hoặc không rõ ràng, hãy liên hệ với người bán để được giải đáp trước khi quyết định mua hàng.
4 điều cần biết khi mua hàng trực tuyến
3
Chính sách khách hàng
Chọn mua hàng từ các sàn thương mại điện tử uy tín và có chính sách chăm sóc khách hàng. Trước khi mua hàng, đọc kỹ chính sách bảo hành và hoàn tiền để biết được quyền lợi của mình trong trường hợp sản phẩm có vấn đề.
4
Phản hồi & đánh giá
Đọc kỹ đánh giá và nhận xét từ người dùng khác về sản phẩm và dịch vụ. Cẩn thận với những bình luận tiêu cực hoặc những bình luận quá tốt lặp đi lặp lại một cách bất thường, thường do người bán/ kênh bán seeding để tăng độ uy tín ảo).

LỪA ĐẢO

ĐÁNH CẮP THÔNG TIN CCCD

DẤU HIỆU NHẬN BIẾT

BIỆN PHÁP PHÒNG TRÁNH

01 Kẻ gian lợi dụng thông tin cá nhân trên CCCD để đăng ký mã số thuế ảo, sau đó sử dụng mã này để thực hiện các hoạt động lừa đảo, gian lận.

02 Các tổ chức tín dụng đen trên cho vay tiền nhanh chóng với lãi suất cao khiến người vay rơi vào cảnh nợ nần, sau đó uy hiếp, dọa dẫm và bôi nhọ danh dự nạn nhân và người thân trên mạng xã hội.

03 Cảnh giác với tin nhắn, cuộc gọi hoặc thông tin từ người không rõ danh tính. Tuyệt đối không chuyển khoản tiền hoặc cung cấp thông tin cá nhân.

04 Giả danh cơ quan công an hoặc tổ chức ngân hàng dọa dẫm chuyển tiền nhanh hoặc yêu cầu cung cấp mã OTP, mật khẩu,... nhằm chiếm đoạt tài sản.

THỦ ĐOẠN CHUYỂN TIỀN NHẦM TÀI KHOẢN NGÂN HÀNG

DẤU HIỆU NHẬN BIẾT

1 CỐ TÌNH CHUYỂN NHẦM TIỀN VÀO TÀI KHOẢN NẠN NHÂN

- GIẢ DANH THU HỒI NỢ ĐỐI KHOẢN VAY +LÃI SẤT CAO

2 - MẠO DANH NGÂN HÀNG THÔNG BÁO CHUYỂN NHẦM, DỤ BẤM VÀO LINK ĐÁNH CẮP THÔNG TIN TÀI KHOẢN

CẦN LÀM GÌ ???

Khi nhận được tiền chuyển khoản nhầm, người nhận cần lưu ý không sử dụng số tiền ấy vào việc chi tiêu cá nhân.

Tuyệt đối không chuyển lại tiền khi không có bên thứ ba làm chứng. Chỉ nên làm việc trực tiếp với ngân hàng.

Nếu nhận được điện thoại từ ngân hàng, cần kiểm tra xem đó có đúng là số điện thoại của ngân hàng hay không.


CÓ LẤY LẠI ĐƯỢC TIỀN BỊ LỪA TRÊN MẠNG KHÔNG ???
LỪA TRONG LỪA
Lấy lại tiền sau khi bị lừa đảo trên mạng có thể rất khó hoặc thậm chí không thể lấy lại được, và việc tìm kiếm dịch vụ lấy lại tiền có thể dẫn đến một hình thức lừa đảo mới.
01
ẨN DANH - GIẢ MẠO
Thường sử dụng các phương tiện và tài khoản ẩn danh hoặc giả mạo để lừa đảo khiến việc xác định danh tính thật sự của đối tượng lừa đảo rất khó khăn và phức tạp.
02
LỪA ĐẢO XUYÊN BIÊN GIỚI
Thường diễn ra trên phạm vi quốc tế và đối tượng cũng có thể là công dân của nhiều quốc gia khác nhau. Điều này làm cho việc truy tìm, theo dõi và xử lý pháp lý trở nên khó khăn và gặp rất nhiều trở ngại pháp lý.
03
THANH TOÁN KHÔNG AN TOÀN
Thường sử dụng các phương tiện thanh toán và ví điện tử có tốc độ giao dịch nhanh chóng. Khi đối tượng lừa được tiền sẽ lập tức chuyển qua nhiều tài khoản khác nhau để xóa dấu vết.
04
DẤU VẾT
Thường không thu thập đủ chứng cứ và dấu vết để điều tra vì đối tượng lừa đảo luôn sử dụng các phần mềm tinh vi để che đậy và xóa dấu vết của các hoạt động lừa đảo.
05
NO!
STOP


LỪA ĐẢO LẤY CẮP
MÃ OTP TRÊN TELEGRAM
Đối tượng lừa đảo có thể giả mạo thành bất cứ ai để tiếp cận bạn!
KẺ LỪA ĐẢO
Chào bạn!
Tôi thấy có một tài khoản Telegram khác giống bạn, có phải bạn dùng hai tài khoản Telegram khác nhau đúng không nhỉ?
Biết số điện thoại của nạn nhân trước khi tiếp cận. Reset mật khẩu để gửi mã OTP về điện thoại của nạn nhân.
Không, tôi chỉ dùng duy nhất tài khoản này thôi. Những tài khoản khác là giả mạo đó!
Lạ nhỉ! Bạn có thể chụp màn hình tài khoản của bạn cho tôi xem được không?
Đợi chút để tôi chụp lại cho bạn xem. Hãy tin tôi!
Chỉ cần gửi ảnh chụp màn hình có chứa mã OTP. Bạn có thể mất tài khoản ngay lập tức !!!
KHÔNG GỬI ẢNH CHỤP MÀN HÌNH CHỨA MÃ OTP
Khi chụp màn hình rất dễ bị dính mã OTP trên thông báo đẩy của điện thoại !!!
Telegram code: xxxx
You can also tap on this link to confirm your new number: https://t.me/login/xxxx
Báo cáo ngay đến Support của Telegram để khóa/ chặn tài khoản lừa đảo đó !

LỪA ĐẢO
TUNG TIN GIẢ VỀ CUỘC GỌI MẤT TIỀN

Thông tin về việc chỉ bằng việc nhận cuộc gọi voicecall bạn có thể bị mất tiền như FlashAI hoặc tương tự là **KHÔNG** chính xác.

Người dùng không thể bị trừ tiền chỉ bằng việc nhận cuộc gọi voicecall thông thường trên điện thoại di động. Các hành động này chỉ nhằm mục đích câu views, likes và gây hoang mang dư luận xã hội.

NHẬN DIỆN VÀ PHÒNG TRÁNH

SỐ ĐIỆN THOẠI LẠ

Bạn nên cảnh giác và tránh tiếp nhận các cuộc gọi không mong muốn từ các số điện thoại lạ, đặc biệt là từ các số không rõ nguồn gốc.

1

GIẢ MẠO SỐ ĐIỆN THOẠI

Có một số hình thức lừa đảo, như "cướp cuộc gọi" (call spoofing) hay "vishing", trong đó kẻ gian sẽ giả mạo số điện thoại hoặc sử dụng các công nghệ để hiển thị số điện thoại khác khi gọi đến.

2

THAO TÚNG TÂM LÝ

Mục đích của chúng là lừa đảo người dùng bằng cách thuyết phục họ THAO TÁC theo hướng dẫn của kẻ lừa đảo để tiết lộ thông tin cá nhân, mật khẩu hoặc thực hiện các giao dịch tài chính.

3

TRẢ LỜI TỈNH TÁO

Nếu bạn nhận được cuộc gọi không mong muốn, hãy cẩn thận và không tiết lộ thông tin cá nhân hay tài khoản của mình.

4

LỪA ĐẢO
DỊCH VỤ LẤY LẠI FACEBOOK

MẤT TÀI KHOẢN FACEBOOK

TÌM KIẾM DỊCH VỤ LẤY LẠI FACEBOOK BỊ MẤT

MẤT THÔNG TIN CÁ NHÂN HOẶC BỊ LỪA MẤT TIỀN

Facebook không kiểm chứng và bảo hộ cho những dịch vụ lấy lại tài khoản bị mất

LÀM GÌ ??? BẢO VỆ FACEBOOK

1. **Sử dụng mật khẩu mạnh**
2. **Bật xác thực hai bước**
3. **Kiểm tra lịch sử đăng nhập**
4. **Hạn chế quyền truy cập**
5. **Tiêu chuẩn cộng đồng và chính sách bảo mật**
6. **Cập nhật phiên bản mới**
7. **Tránh bị lừa đảo và phishing**
8. **Liên kết và tập tin đính kèm**
9. **Tắt tính năng đăng nhập tự động**
10. **Không chia sẻ mật khẩu**

LỪA ĐẢO

TÌNH CẢM

DẤU HIỆU NHẬN BIẾT

Xác định, tiếp cận và xây dựng mối quan hệ với nạn nhân.

Dẫn dụ nạn nhân gửi hình ảnh, video nhạy cảm.

Đe dọa, lừa đảo hoặc chiếm đoạt tài sản, tống tiền.

BIỆN PHÁP PHÒNG TRÁNH

* Hãy giữ cảnh giác và không quá nhanh tin tưởng vào một người mới gặp qua mạng xã hội hoặc các nền tảng trực tuyến khác.

* Khi gặp một người mới trên mạng xã hội hoặc các nền tảng trực tuyến, hãy xác minh danh tính của họ.

* Cẩn trọng khi chia sẻ hình ảnh và video nhạy cảm.

* Hãy cảnh giác với những yêu cầu gửi tiền, đầu tư hoặc tham gia các giao dịch tài chính không rõ nguồn gốc.

* Cảnh giác với các cuộc gọi trúng thưởng và đào sâu các kiến thức về đầu tư tài chính.

* Kiểm tra thông tin trước khi nhận hàng bưu kiện của một người không quen biết.

* Nắm vững kiến thức về các hình thức lừa đảo phổ biến và cách nhận diện các dấu hiệu đáng ngờ.

* Bảo vệ thông tin cá nhân bằng cách không chia sẻ quá nhiều thông tin trên mạng xã hội hoặc các nền tảng trực tuyến.

* Hãy giữu bình tĩnh và đặt sự an toàn cá nhân lên hàng đầu.

RẢI PHISHING LỪA ĐẢO QUẢNG CÁO BẨN TRÊN FACEBOOK

DẤU HIỆU NHẬN BIẾT

Tạo một trang web giả mạo

- Kẻ lừa đảo tạo một trang web giả mạo có giao diện tương tự như một trang web đáng tin cậy như ngân hàng hoặc dịch vụ trực tuyến.
- Trang web này được thiết kế để thu thập thông tin cá nhân và đăng nhập của người dùng khi họ nhập vào.

Rải link và seeding quảng cáo bẩn trên Facebook

- Kẻ lừa đảo sử dụng các tài khoản giả mạo hoặc các tài khoản đã bị xâm nhập để rải link và seeding quảng cáo bẩn trên Facebook.
- Spam bài viết, nhận xét, bình luận hoặc quảng cáo với đường link đã được tạo, hấp dẫn người dùng để nhấn vào.

Tạo một đường link hấp dẫn

- Tạo một đường link hấp dẫn sử dụng tiêu đề hoặc mô tả mà người dùng quan tâm như "Nhận ngay ưu đãi đặc biệt" hoặc "Kiểm tra tài khoản của bạn" hoặc các sự kiện đang hot trending trên mạng xã hội.
- Đường link có vẻ giả giống như một đường link đáng tin cậy nhằm tránh bị phát hiện.

Lừa đảo và đánh cắp thông tin, tài sản

- Khi người dùng nhấn vào đường link lừa đảo, nạn nhân sẽ chuyển hướng đến trang web phishing mà kẻ lừa đảo đã tạo sẵn.
- Từ đó, kẻ lừa đảo có thể thu thập thông tin cá nhân, tài khoản hoặc đăng nhập của họ và sử dụng để lừa đảo hoặc đánh cắp tài sản.

BIỆN PHÁP PHÒNG TRÁNH

01 Cẩn thận với các đường link không rõ nguồn gốc

02 Kiểm tra địa chỉ URL trước khi nhấp vào

03 Đánh giá tính xác thực của quảng cáo, tin nhắn, bình luận

04 Tăng cường bảo mật tài khoản

05 Tìm hiểu về các hình thức lừa đảo và phishing

06 Cẩn trọng với việc chia sẻ thông tin cá nhân

07 Cập nhật phiên bản mới nhất của trình duyệt và phần mềm bảo mật

08 Báo cáo các trường hợp đáng ngờ khi phát hiện các link phishing

09 Giáo dục và nâng cao nhận thức về các hình thức lừa đảo phổ biến

10 Sử dụng phần mềm chống malware và chống phishing để bảo vệ thiết bị

LỪA ĐẢO
CHO SỐ ĐÁNH LÔ ĐỀ

Đánh số lô, số đề trên mạng xã hội với các dấu hiệu như phải đóng phí trước, rủi ro mất phí khi không trúng, và phải chia hoa hồng khi trúng là một *HÌNH THỨC LỪA ĐẢO* nguy hiểm.

DẤU HIỆU NHẬN BIẾT

Kẻ lừa đảo tiếp cận người khác thông qua các phương tiện như điện thoại, email, tin nhắn hoặc mạng xã hội. Họ quảng cáo về việc cung cấp số lô, số đề may mắn có khả năng trúng thưởng lớn.

Sau khi người khác đã đóng phí, kẻ lừa đảo cung cấp các số lô, số đề cho người đó đánh. Họ tạo ra cảm giác rằng những số này sẽ mang lại kết quả trúng thưởng lớn.

Kẻ lừa đảo sử dụng các câu chuyện thành công, chứng cứ giả và những lời tán tụng để tạo niềm tin và thuyết phục người khác rằng họ có khả năng đưa ra các số lô, số đề chính xác.

Trong trường hợp người khác không trúng thưởng, kẻ lừa đảo không trả lại số tiền phí mà người khác đã đóng trước đó. Họ sử dụng lý do rằng đó là một khoản phí không hoàn lại hoặc chi phí liên quan đến việc cung cấp các số lô, số đề.

Kẻ lừa đảo yêu cầu người khác đóng một khoản phí trước để nhận được các số lô, số đề may mắn. Họ thường đưa ra lý do như phí dịch vụ, phí tiền trí hoặc phí đăng ký.

Nếu người khác trúng thưởng, kẻ lừa đảo yêu cầu người đó chia hoa hồng hoặc trả một phần tiền thưởng cho mình dưới danh nghĩa đã cung cấp các số lô, số đề may mắn.

BIỆN PHÁP PHÒNG TRÁNH

1. KHÔNG TIN VÀO LỜI HỨA DỄ DÀNG KIẾM TIỀN
2. KHÔNG ĐÓNG PHÍ TRƯỚC
3. KIỂM TRA TÍNH XÁC THỰC CỦA NGUỒN TIN
4. TRÁNH VIỆC CHIA HOA HỒNG KHI TRÚNG
5. BÁO CÁO SỰ VIỆC KHI GẶP NHỮNG HÌNH THỨC NÀY

Việc tham gia vào các hoạt động không rõ nguồn gốc và không đáng tin cậy như đánh số lô, số đề trên mạng xã hội có thể gây mất tiền bạc và hậu quả pháp lý nghiêm trọng. Hãy cẩn thận, cân nhắc và tìm hiểu kỹ trước khi quyết định tham gia bất kỳ hoạt động tài chính nào để bảo vệ tài sản và tránh trở thành nạn nhân của lừa đảo trực tuyến.

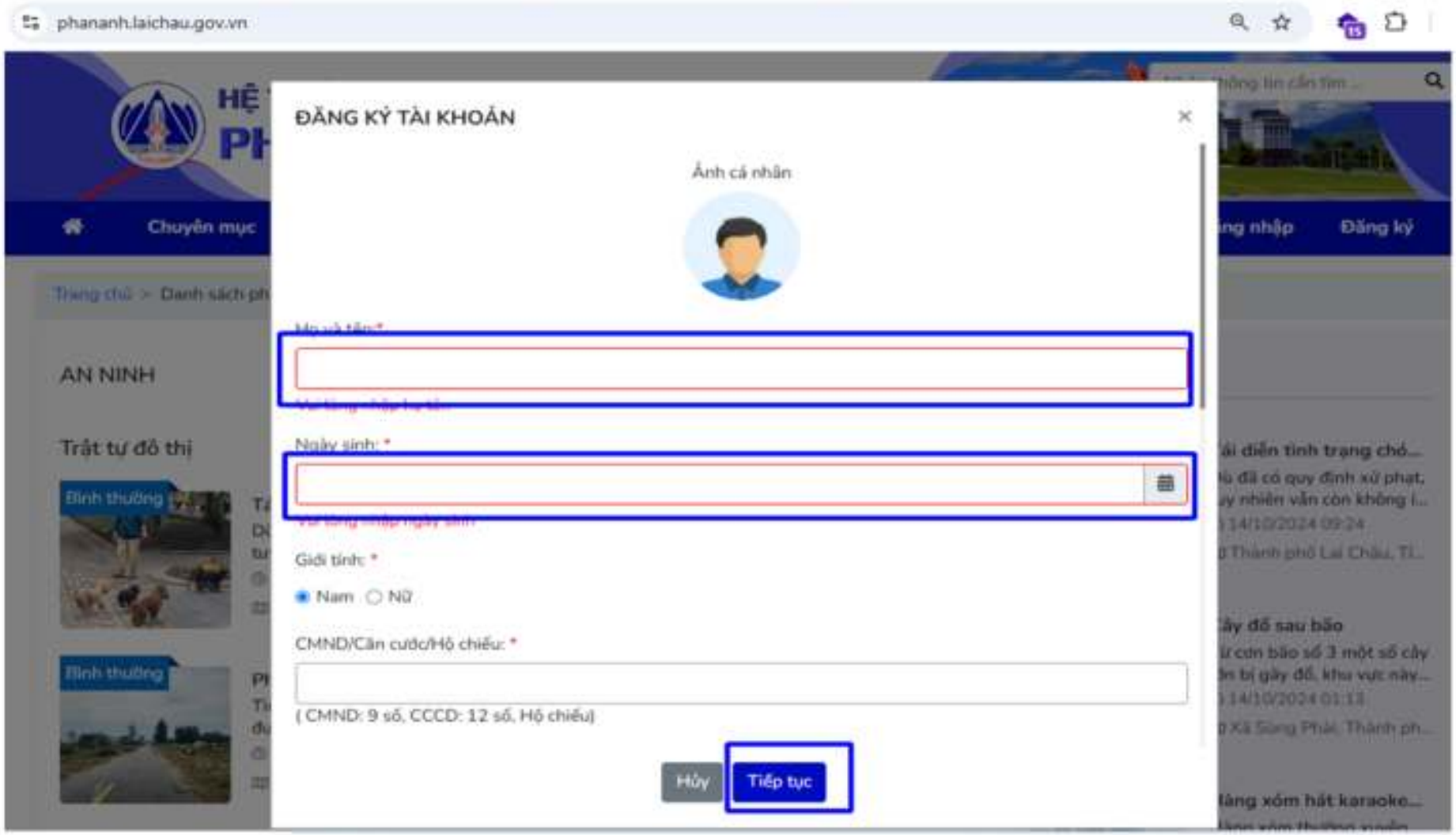
CỔNG THÔNG TIN TƯƠNG TÁC PHẢN ÁNH HIỆN TRƯỜNG

(Địa chỉ Website: https://phananh.laichau.gov.vn)

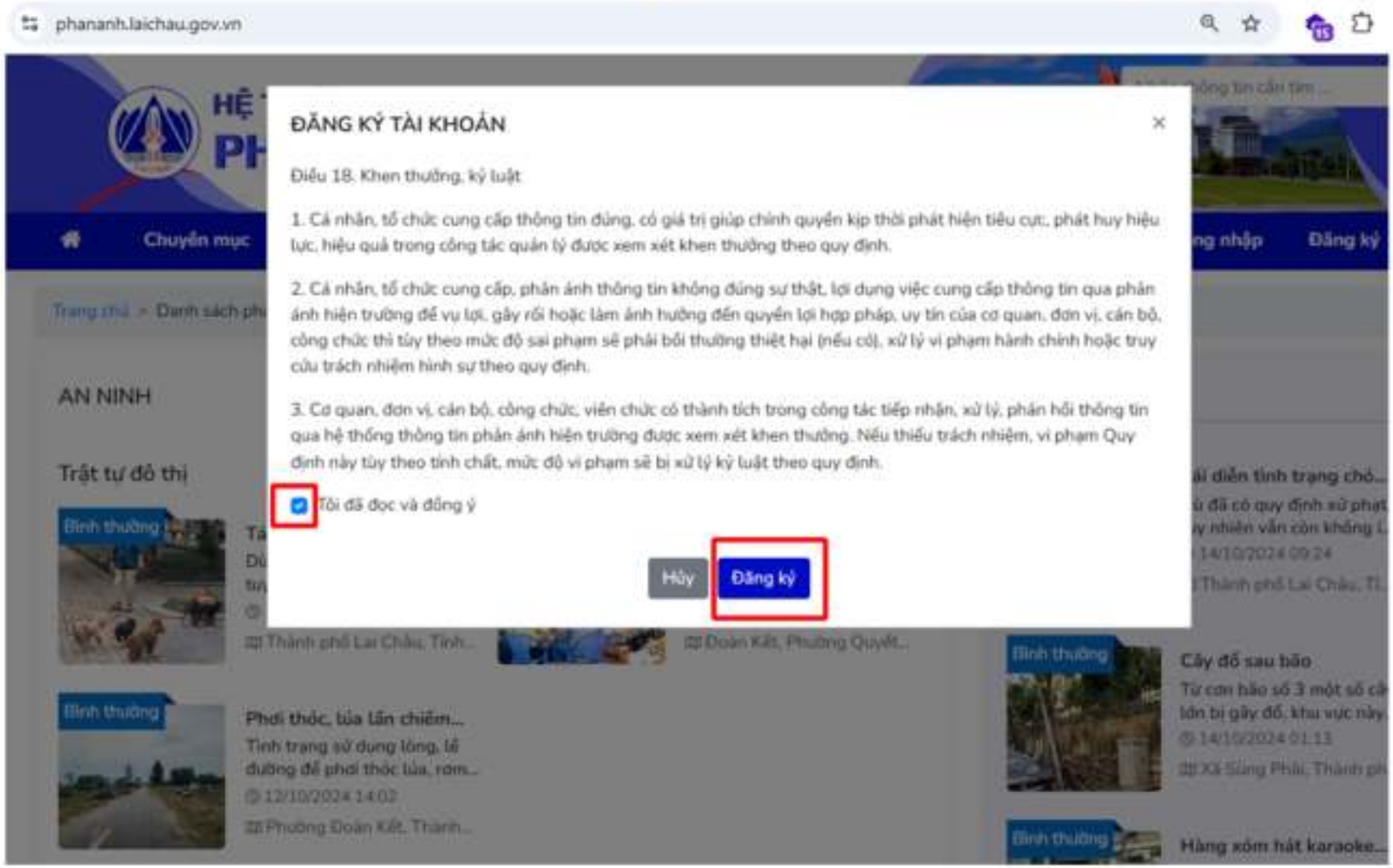
1. Đăng ký tài khoản

Bước 1: Tại màn hình trang chủ, nhấn "Đăng ký"

Bước 2: Nhập đầy đủ thông tin, các trường * bắt buộc và nhấn "Tiếp tục"



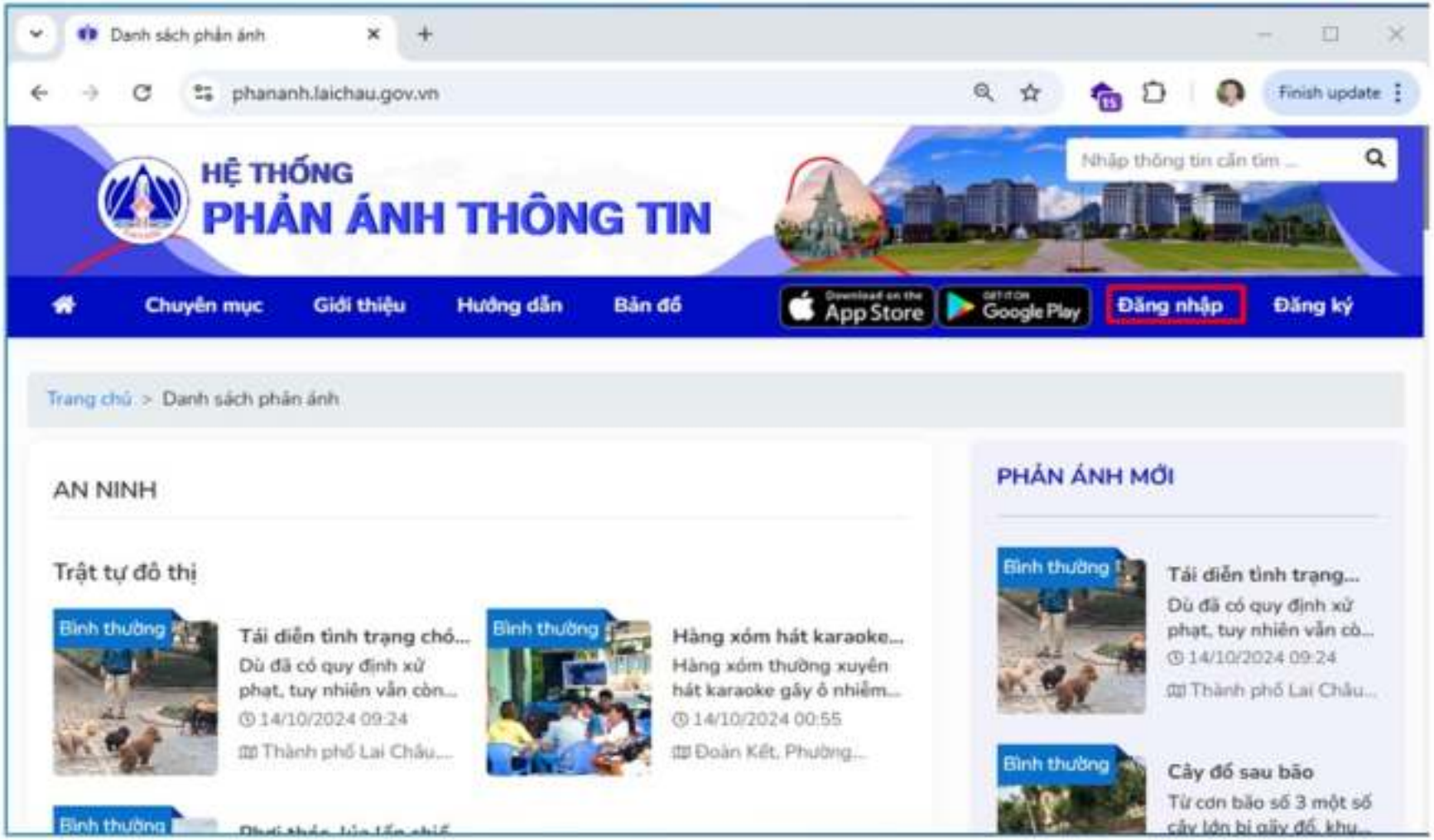
Bước 3: Nhấn "Tôi đã đọc và đồng ý" sau đó Chọn "Đăng ký"



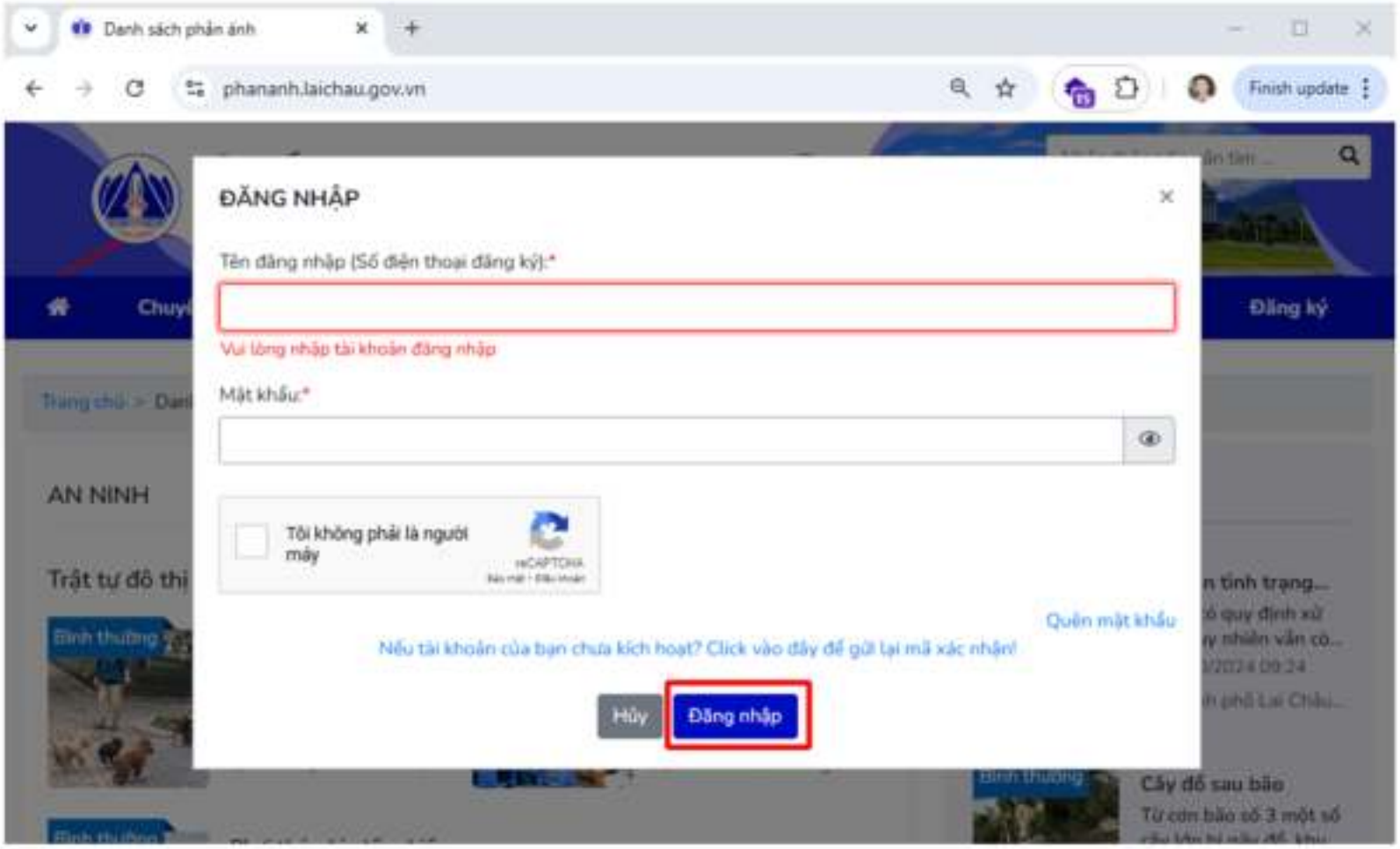
Bước 4: Nhập mã xác thực đã được gửi qua Số điện thoại đăng ký và chọn "Xác nhận"

2. Đăng nhập tài khoản

Bước 1: Tại màn hình trang chủ, nhấn "Đăng nhập"



Bước 2: Nhập đầy đủ thông tin, nhấn **Đăng nhập**

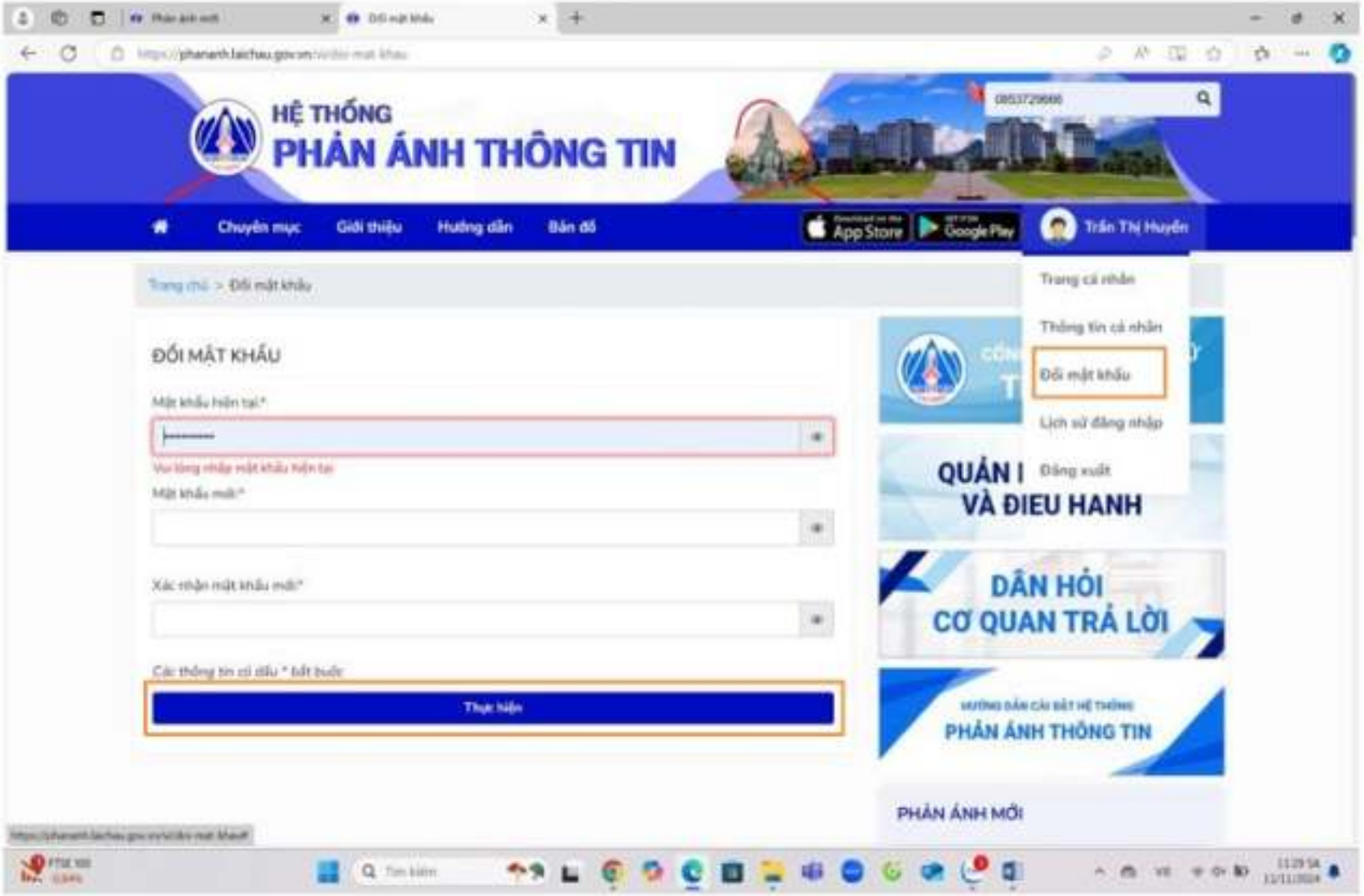


3. Thiết lập tài khoản

Bước 1: Nhấn vào hình  và Chọn " Thông tin cá nhân"

Bước 2: Để chỉnh sửa thông tin tài khoản, người dùng thực hiện đổi thông tin và chọn "Cập nhật"

Bước 3: Để đổi mật khẩu, người dùng chọn "Đổi mật khẩu" => chọn "Thực hiện"



4. Đăng xuất tài khoản

Bước 1: Nhấn vào hình  và Chọn " Đăng xuất"

5. Gửi phản ánh

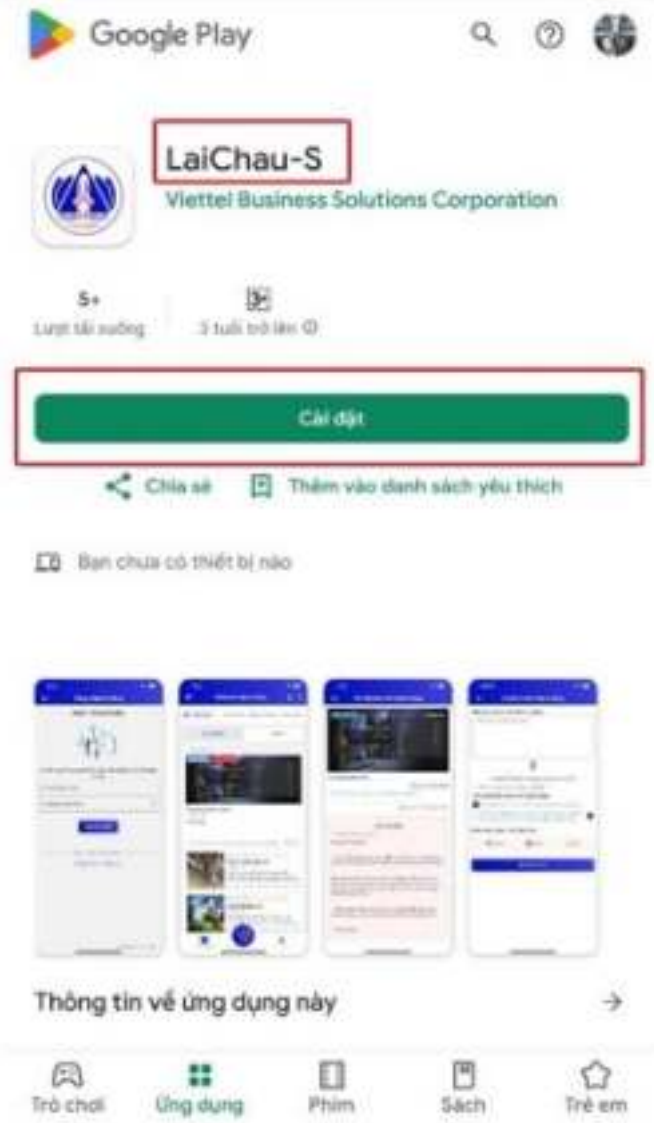
Tại Trang chủ màn hình đã hiển thị giao diện để Gửi phản ánh. Để gửi phản ánh người dùng điền đầy đủ nội dung góp ý, thêm hình ảnh và Gửi phản ánh

ỨNG DỤNG LAICHAU-S
PHẢN ÁNH HIỆN TRƯỜNG

Điện thoại hệ điều hành Android thì chọn Google Play
Điện thoại hệ điều hành iOS thì chọn App Store

1. Cài đặt ứng dụng trên nền tảng IOS

2. Cài đặt ứng dụng trên nền tảng Android



3. Đăng ký tài khoản

Mở ứng dụng và thực hiện theo các bước sau đây:

Bước 1

Bước 2

Bước 3

Bước 4

Bước 5

Bước 6

Bước 7

LƯU Ý:

- ✓ Mỗi số điện thoại chỉ được đăng 1 lần.
- ✓ Mật khẩu phải có tối thiểu 8 ký tự (bao gồm chữ hoa, chữ thường, chữ số và ký tự đặc biệt).
- ✓ Tài khoản phải kích hoạt rồi mới được đăng nhập.

4. Đăng nhập tài khoản

Mở ứng dụng và thực hiện theo các bước sau đây:

Bước 1

Bước 2

Bước 3

5. Xem thông tin tài khoản

- ✓ **Bước 1:** Đăng nhập thành công vào hệ thống.
- ✓ **Bước 2:** Nhấn vào hình avatar hoặc icon "Cá nhân".

Giao diện thông tin cá nhân như hình bên.

6. Chỉnh sửa thông tin tài khoản

Bước 1: Tại giao diện Thông tin cá nhân, nhấn "Chỉnh sửa thông tin"

Bước 2: Nhập các thông tin cần chỉnh sửa, nhấn "Cập nhật"

7. Đăng xuất tài khoản

Bước 1: Nhấn biểu tượng "Đăng xuất", chọn "Tài khoản cộng đồng"

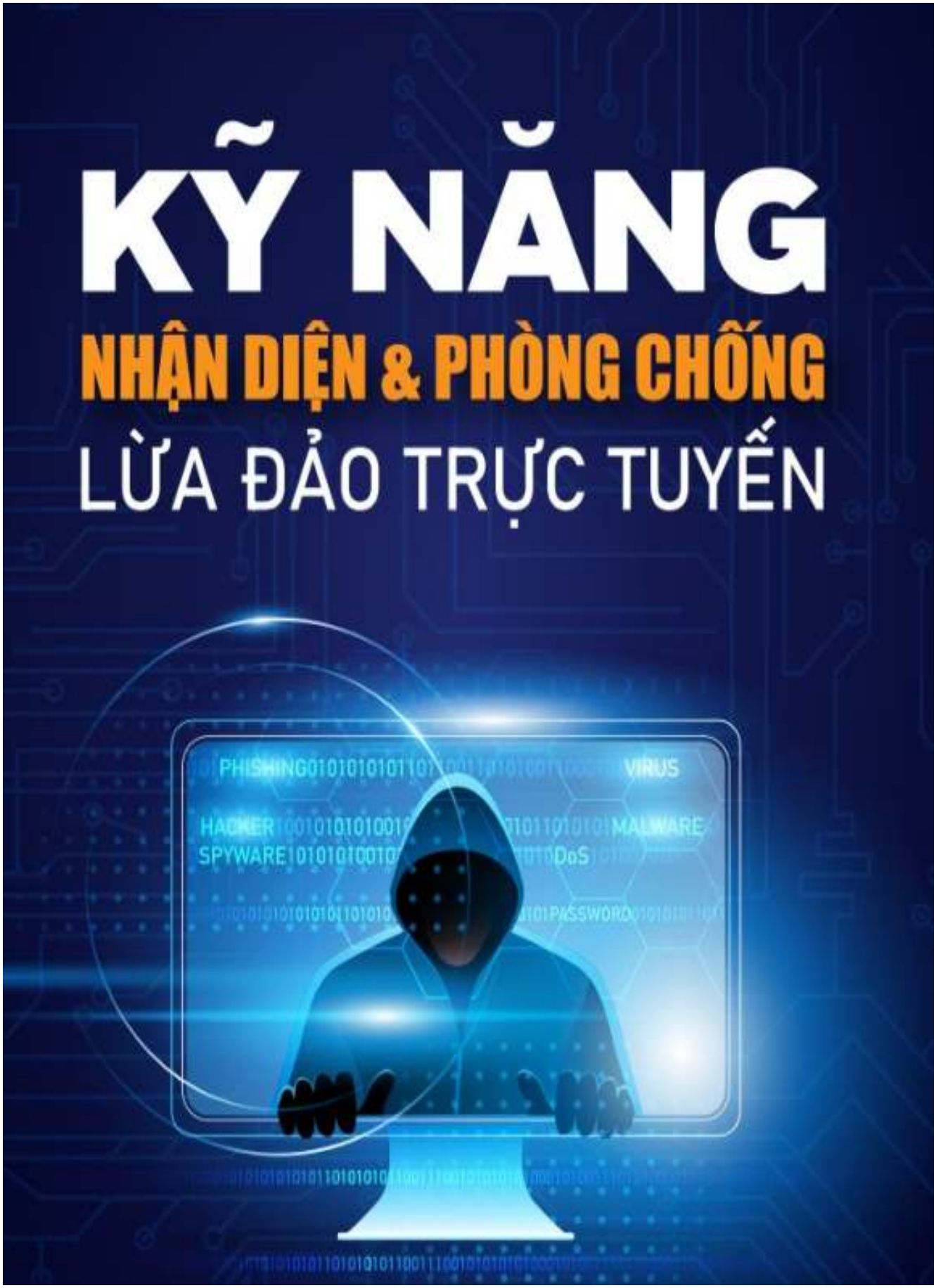
Bước 2: Nhấn nút "Đăng xuất"

8. Gửi phản ánh

- ✓ **Bước 1:** Nhấn biểu tượng  để chọn chức năng phản ánh hiện trường
- ✓ **Bước 2:** Nhấn biểu tượng  để mở giao diện tạo phản ánh.

Bước 3: Nhấn biểu tượng để tạo phản ánh.

Bước 4: Nhập các thông tin và nhấn "Gửi phản ánh".


KỸ NĂNG
NHẬN DIỆN & PHÒNG CHỐNG
LỪA ĐẢO TRỰC TUYẾN
PHISHING
VIRUS
HACKER
MALWARE
SPYWARE
DoS
PASSWORD


NÂNG CAO NHẬN THỨC VÀ PHÒNG TRÁNH LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG CHỈ TRONG 3 BƯỚC
TẠM DỪNG
Đối tượng lừa đảo thường nguỵ tạo ra các tình huống khẩn cấp để dẫn dắt nạn nhân hành động bốc đồng. Khi bạn nhìn thấy một tin nhắn, email hoặc liên kết đáng ngờ, hãy tạm ngừng lại. Không truy cập, phản hồi hoặc cung cấp bất kỳ thông tin nào.
SUY NGHĨ
Tìm hiểu kỹ nội dung, thông tin: lỗi chính tả, địa chỉ người gửi không quen thuộc. Để ý các yêu cầu, đề nghị bất thường như yêu cầu thông tin cá nhân. Ví dụ: ngân hàng và cơ quan nhà nước không làm việc với người dân qua điện thoại.
QUYẾT ĐỊNH
Tuyệt đối không truy cập liên kết hoặc phản hồi lại trừ khi bạn xác nhận tin nhắn an toàn. Báo cáo tin nhắn lừa đảo với quản trị viên của hệ thống.

4 ĐIỀU CẦN LÀM NGAY KHI GẶP LỪA ĐẢO TRỰC TUYẾN

BÁO CÁO TIN NHẮN, CUỘC GỌI RÁC

Báo cáo các tài khoản có dấu hiệu gửi tin nhắn lừa đảo trên các nền tảng mạng xã hội. Báo cáo số điện thoại của đối tượng lừa đảo với cơ quan công an.

CHỦ ĐỘNG CHẶN LIÊN HỆ

Khi bị tiếp cận bởi các tin nhắn, cuộc gọi có dấu hiệu lừa đảo, người dân nên chủ động ngắt liên lạc, chặn các liên hệ có hành vi trên.

TRA CỨU THÔNG TIN TRÊN MẠNG

Tra cứu các thông tin liên quan tới hành vi lừa đảo đã được báo cáo và đăng tải bởi các cơ quan truyền thông hoặc nạn nhân khác. Cập nhật các phương thức thủ đoạn người dân mới gặp phải cho cơ quan chức năng.

GỬI CẢNH BÁO CHO NCSC

Gửi cảnh báo về Trang cảnh báo an toàn thông tin Việt Nam - Trung tâm Giám sát an toàn không gian mạng quốc gia tại địa chỉ: https://canhbao.khonggianmang.vn

5 ĐIỀU CẦN LÀM SAU KHI BỊ LỪA CHUYỂN TIỀN QUA MẠNG

1. Dừng chuyển tiền

Các đối tượng lừa đảo sử dụng nhiều thủ đoạn dẫn dắt nạn nhân chuyển tiền liên tục nhiều khoản tiền từ nhỏ đến lớn. Nạn nhân cần dừng chuyển tiền càng sớm càng tốt để giảm thiểu thiệt hại.

2. Liên hệ với ngân hàng

Người dân cần liên hệ ngay lập tức với ngân hàng và tổ chức tài chính để báo cáo lừa đảo và yêu cầu họ dừng mọi giao dịch đang và sẽ gửi đến đối tượng lừa đảo.

3. Thu thập và lưu lại bằng chứng

Nhanh chóng lưu lại các đoạn hội thoại với đối tượng lừa đảo, lịch sử giao dịch chuyển khoản nhằm phục vụ cho quá trình điều tra và truy vết đối tượng.

4. Trình báo với cơ quan chức năng

Từ các bằng chứng đã thu thập và lưu lại, người dân trình báo vụ việc lừa đảo trực tuyến với các cơ quan công an địa phương.

5. Cảnh báo cho người thân và bạn bè

Người dân thông tin, chia sẻ kinh nghiệm cho người thân, bạn bè trước các thủ đoạn lừa đảo trên không gian mạng đã và đang ngày càng diễn biến phức tạp

BẢO VỆ BẢN THÂN TRÊN
KHÔNG GIAN MẠNG

QUY TẮC 6 "KHÔNG"

1

KHÔNG cung cấp thông tin cá nhân cho người lạ; kiểm tra kỹ thông tin chuyển khoản trước khi thực hiện giao dịch trực tuyến.

2

KHÔNG chấp nhận lời mời kết bạn từ người lạ; cân nhắc kỹ lưỡng trước khi tham gia các hội nhóm trên mạng xã hội.

3

KHÔNG truy cập các đường dẫn, liên kết, website, ứng dụng không rõ nguồn gốc hoặc mở tệp đính kèm đến từ tin nhắn.

4

KHÔNG cơ quan nhà nước nào làm việc qua điện thoại; ngắt kết nối khi có đối tượng tự xưng cán bộ cơ quan nhà nước gọi điện tới.

5

KHÔNG chuyển khoản đặt cọc khi mua hàng trực tuyến.

6

KHÔNG phản hồi lại đối với các đối tượng gửi tin nhắn trúng thưởng, tuyển dụng "việc nhẹ lương cao"