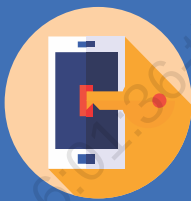




CẨM NANG PHÒNG TRÁNH LỪA ĐẢO TRỰC TUYẾN!



Nội dung cẩm nang

1.	Bảo mật tài khoản	1
2.	Chia sẻ sáng suốt	10
3.	Kết giao chọn lọc	18
4.	Phòng tránh lừa đảo trực tuyến	25

Nội dung: Được tổng hợp, biên tập bởi Phòng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao và Phòng Tham mưu - Công an thành phố Đà Nẵng.

Liên hệ: <https://www.facebook.com/Anninhmang.danang>



Bảo mật 

Tài khoản

1.

1.

Bảo mật Tài khoản



Sử dụng mật khẩu

Tài khoản trực tuyến như tài khoản mạng xã hội, tài khoản ngân hàng... lưu giữ các thông tin cá nhân và tài chính quan trọng, hãy lưu ý các bước sau để giữ bảo mật tối ưu.

-  Sử dụng mật khẩu dài ít nhất **8 ký tự**: gồm chữ hoa, chữ thường, số và ký tự đặc biệt. Dùng mật khẩu dễ nhớ nhưng khó đoán.
-  **Ví dụ:** Chữ cái đầu 1 câu hát yêu thích / 1 câu nói dễ nhớ / đổi chữ thành số...

10 năm phấn đấu để thành công!



10 năm *phấn* *đấu* *để* thành *công*!



10npddtc!



* * *

1.

Bảo mật

tài khoản 



Xác minh 2 bước



Google

Xác minh 2 bước (còn gọi là xác thực hai yếu tố), bạn có thể thêm một lớp bảo mật nữa vào tài khoản của bạn để phòng trường hợp mật khẩu của bạn bị đánh cắp.

- ✓ Mở **tài khoản Google**, trong bảng điều hướng, hãy chọn mục **Bảo mật**. Trong phần "Cách bạn đăng nhập vào Google", hãy chọn:
- ✓ **Xác minh 2 bước** → **Bắt đầu**. Và làm theo các bước trên màn hình.



Xác nhận 2 bước



Nhập tên người dùng và mật khẩu



Nhập mã xác thực một lần được gửi qua ứng dụng hoặc tin nhắn SMS.

Google

Có phải bạn đang cố đăng nhập?



Anhphan@gmail.com

Chromebook

Việt Nam

Không

Đúng là tôi

1.

Bảo mật

Tài khoản



Xác minh 2 bước 

facebook

- ✓ Đi đến phần **Cài đặt** → **bảo mật và đăng nhập**. Cuộn xuống phần **Sử dụng xác thực 2 yếu tố** và nhấp vào **Chỉnh sửa**.
- ✓ Chọn phương thức bảo mật: [Gợi ý] → Mã nhận qua tin nhắn văn bản (SMS) trên điện thoại di động. Rồi làm theo hướng dẫn trên màn hình.

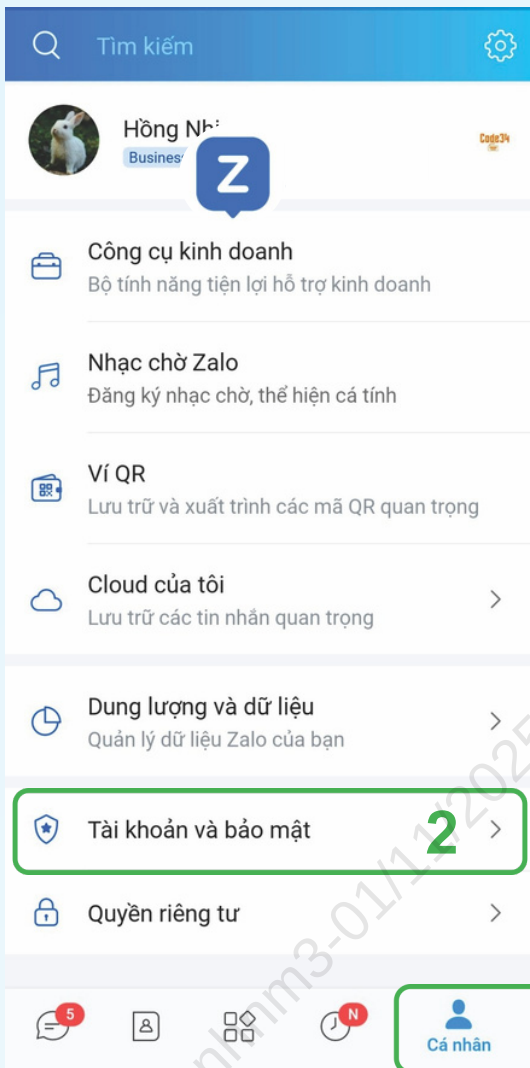


1.

Bảo mật Tài khoản



Xác minh 2 bước ✓



✓ Mở ứng dụng Zalo trên thiết bị → nhấn vào tab **Cá nhân** chạm vào biểu tượng **bánh răng cài đặt** → nhấn vào **Tài khoản và bảo mật**

✓ **Bật công tắc chuyển đổi tại Bảo mật 2 lớp.**

Đăng nhập

3

Bảo mật 2 lớp



Thêm hình thức xác nhận để bảo vệ tài khoản khi đăng nhập trên thiết bị mới



1.

Bảo mật

Tài khoản



Không nên

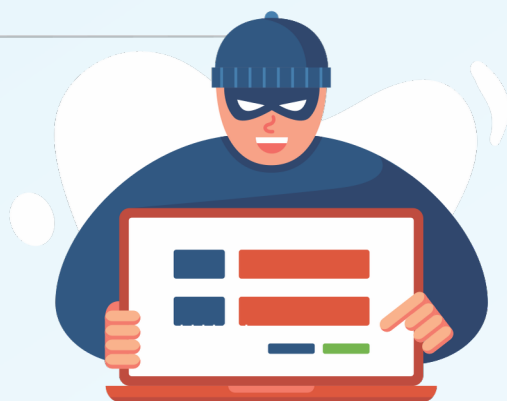
 Không đặt **mật khẩu đơn giản như** tên, ngày sinh, số điện thoại hay các thông tin dễ đoán khác...

Password

08071952



 Không chia sẻ **thông tin đăng nhập** và **mật khẩu** cho người khác hoặc để ở nơi dễ nhìn thấy.



 Không truy cập **trang web không tin cậy**, không tải, cài đặt các phần mềm, ứng dụng ngoài các kho ứng dụng trực tuyến uy tín như Google Play , App Store 



* Góc thử thách



1. Hãy cho biết đâu là một khẩu mạnh nhất. Vì sao?

- a. toiyeuquetoit 123
- b. LinhDan98
- c. 1Votrad@ (một vòng trái đất)

2. Một khẩu mạnh gồm những ký tự nào?

- a. Chữ in hoa (A, B, C, ...)
- b. Chữ thường (a, b, c, ...)
- c. Chữ số (1, 2, 3, ...)
- d. Ký tự đặc biệt (@, #, \$, !, ...)
- e. Tất cả các đáp án trên

Ừm và câu 2 e

Câu 1 c nhỉ?

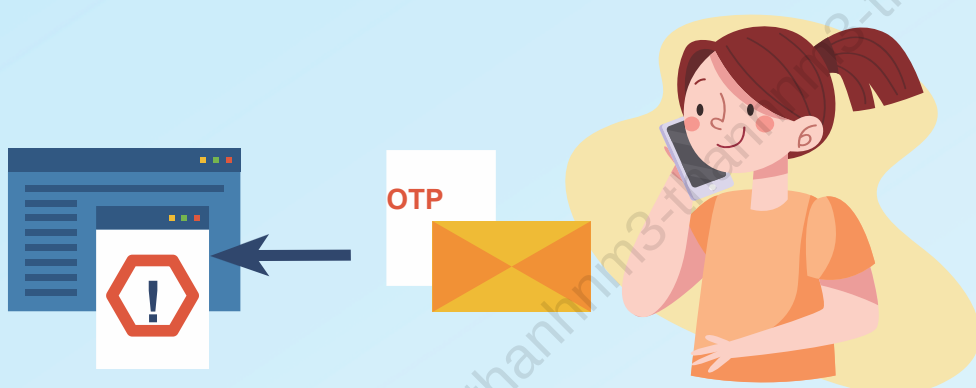


* Góc thử thách



Tác dụng của mật khẩu 2 lớp!

Tớ nhận được thông báo ai đó muốn đổi mật khẩu tài khoản của tớ. Gửi mã OTP về số điện thoại kêu tớ nhập vào nếu tớ là người đổi mật khẩu?



KHÔNG CUNG CẤP MÃ OTP CHO BẤT KỲ AI NHẤT LÀ QUA CUỘC GỌI HOẶC TIN NHẮN



Có thể người đó đã có được mật khẩu của cậu. Đừng lo, mã OTP đừng cung cấp cho ai. Không có mã đó, họ không đăng nhập được đâu. Cậu vào tài khoản đổi lại mật khẩu cho yên tâm nhé!

* Góc tình huống

Tác dụng của mật khẩu 2 lớp!

Ôi trời, mình lỡ nhập tài khoản và mật khẩu Gmail vào trang trúng thưởng giả. Giờ phải làm sao?



<http://trungtang.9999.zdfdf>

Tài khoản: Thnhi@gmail.com

Mật khẩu: 123456

Tức thật! Lấy được tài khoản, mật khẩu bắt nhập mã OTP . Không thể đăng nhập được!!!



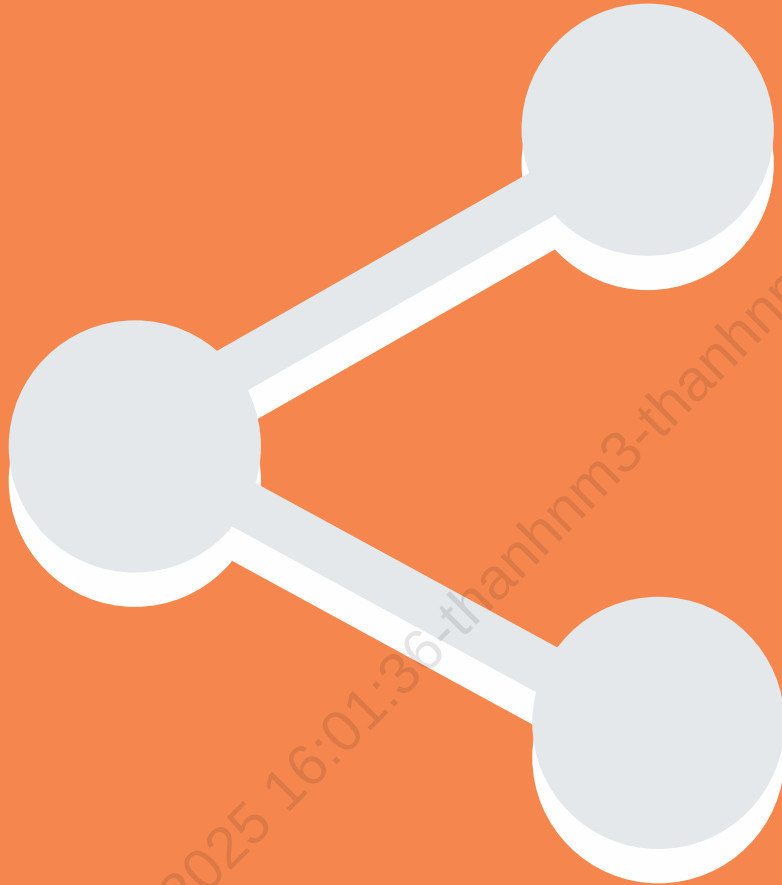
Nhập mã

Để giữ an toàn cho tài khoản của bạn, Google muốn đảm bảo rằng bạn chính là người đang cố đăng nhập

Chúng tôi vừa gửi một tin nhắn văn bản gồm mã xác minh 6 chữ số đến 093xxxxx17

Tiếp theo





2. Chia sẻ

Sáng suốt

2.

Chia sẻ Sáng suốt 💡



Chia sẻ thông tin là một phần không thể thiếu trong cuộc sống. Tuy nhiên, hãy lưu ý một số điều sau đây để an toàn trong chia sẻ thông tin trực tuyến:

2.1. Hãy cân nhắc kỹ về thông tin bạn muốn chia sẻ

Đặc biệt **thận trọng** khi chia sẻ thông tin cá nhân trên mạng và chia sẻ với người khác, bao gồm:



2.

Chia sẻ Sáng suốt 💡



2.2. Sáng suốt với người mình đang chia sẻ cùng

Nên phân cấp chia sẻ ✔️



Với tất cả mọi người

- ✔️ Chia sẻ những nội dung **giải trí lành mạnh, thông tin chính thống hữu ích** cho cộng đồng.
- ✔️ Chia sẻ những thông tin khẩn từ các kênh truyền thông chính thống (về thiên tai, dịch bệnh...)
- ✔️ Đánh giá sản phẩm, dịch vụ, đưa ra ý kiến chia sẻ, giúp người khác có lựa chọn phù hợp...



2.

Chia sẻ Sáng suốt💡



2.2. Sáng suốt với người mình đang chia sẻ cùng

Nên phân cấp chia sẻ ✓



Với gia đình, người thân và bạn bè



Những hình ảnh và video về bản thân, gia đình



Giữ cho riêng mình



Các thông tin cá nhân, lịch trình, tài liệu quan trọng, thông tin tài chính v.v...



2.

Chia sẻ Sáng suốt💡



2.2. Sáng suốt với người mình đang chia sẻ cùng

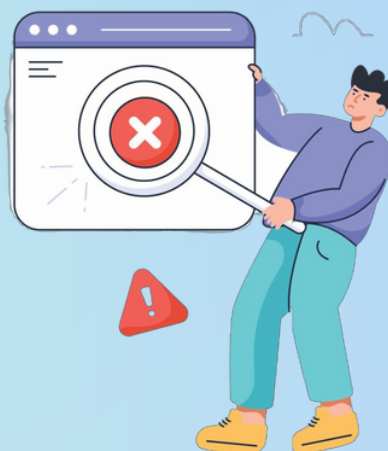
Không nên !

Chia sẻ, đăng tải:

! Thông tin chưa được xác thực, kiểm chứng bởi cơ quan chức năng như tin về an ninh trật tự, chính trị, kinh tế, dịch bệnh, thiên tai...



! Thông tin cá nhân của người khác mà chưa xin phép, như hình ảnh, tên, tuổi, địa chỉ, số điện thoại, việc làm ...



2.

Chia sẻ Sáng suốt💡



2.2. Sáng suốt với người mình đang chia sẻ cùng

Không nên 

Chia sẻ, đăng tải:

- ❗ Thông tin nội bộ doanh nghiệp, tổ chức lên mạng như bí mật kinh doanh, cơ sở dữ liệu, thông tin nhân sự...



- ❗ Nội dung công kích, bôi nhọ danh dự, nhân phẩm cá nhân, tổ chức, như **văng tục, chê bai ngoại hình, phát tán tin đồn** về người khác, đe dọa dùng vũ lực...



Những hành vi trên có thể biến bạn thành người vi phạm pháp luật

2.

Chia sẻ Sáng suốt💡



2.2. Sáng suốt với người mình đang chia sẻ cùng

Khi chia sẻ trực tuyến, thông tin của bạn có thể được lan toả trên số đông cộng đồng mạng. Hãy suy xét kỹ trước khi chia sẻ những nội dung sau

Suy xét kỹ ⚠️

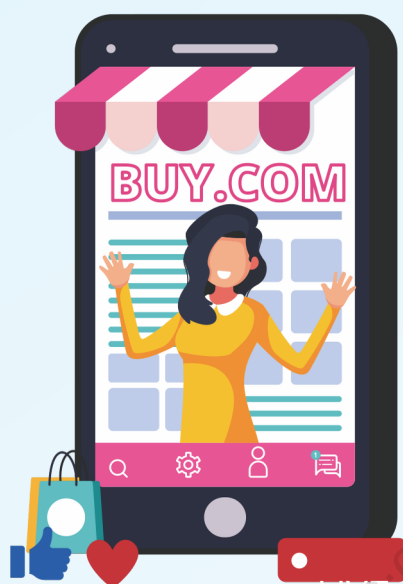
- ⚠️ Tác dụng của **thực phẩm chức năng**
- ⚠️ Công thức bài thuốc dân gian, công thức **phối trộn mỹ phẩm** ...
- ⚠️ Các phương pháp chăm sóc sức khỏe, làm đẹp và **trị liệu tại gia**.



Trước khi chia sẻ, hãy tự hỏi bạn đã thật sự am hiểu tường tận về điều bạn nói? Và trách nhiệm của chúng ta nếu có hậu quả xảy ra khi người khác nghe theo và áp dụng?

* Góc tình huống

Chị A xem “livestream” (phát sóng trực tiếp) mua hàng trên mạng xã hội, người bán yêu cầu ai muốn đặt hàng thì để lại địa chỉ cũng như số điện thoại của mình trong phần bình luận.



Theo bạn có nên?

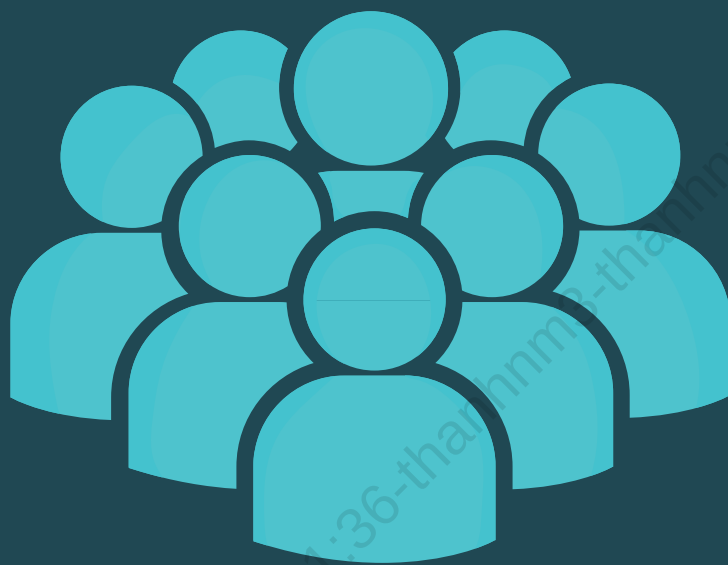


Đ.T.A

- Sđt: 098xxxxxxx

- Đ/c: 15 đường XX, Quận YY...

Không nên chút nào! Vì những kẻ gian có thể giả mạo người bán gọi cho bạn lừa chuyển tiền. Thậm chí, trò lừa tình vì hơn khi họ mạo danh người bán gửi hàng giả về địa chỉ bạn cung cấp để lấy tiền.



3.

Kết giao 

Chọn lọc

3.

Kết giao

Chọn lọc



Kết giao trên mạng không chỉ duy trì các mối quan hệ ngoài đời thực, mà còn là môi trường lý tưởng để tìm kiếm, phát triển những mối quan hệ mới, những tình bạn xuyên biên giới

Tuy nhiên, vẫn nên cẩn trọng để tránh những mối quan hệ độc hại, hay kết giao nhầm với các loại tội phạm lừa đảo



Đặt ra một vài câu hỏi cho bản thân trước khi kết bạn với ai đó trên mạng xã hội.

- Mình có quen biết người này không? Giữa mình và họ có bạn chung không?
- Giữa mình và họ có điểm chung nào? Cùng hội, nhóm nào, cùng quan điểm, sở thích gì?
- Tài khoản thật hay ảo? Bài đăng của họ trên trang cá nhân có thật không, cách họ tương tác với bạn bè?
- Mục đích kết bạn với người này để làm gì?

3.

Kết giao

Chọn lọc



Lời khuyên cho bạn

 Không nhất thiết phải kết bạn thật nhiều, hãy “dọn dẹp” các mối quan hệ không cần thiết.

 Dành thời gian vun đắp cho những mối quan hệ thực sự đáng giá thay vì những con số “ảo” trong danh mục bạn bè.



 Thận trọng, tìm hiểu kỹ thông tin trước khi kết bạn hoặc tham gia các hội, nhóm trên mạng xã hội.

 Hủy kết bạn với người khác, hủy tham gia nhóm khi cảm thấy thông tin của người, nhóm đó không phù hợp với lợi ích cộng đồng.



3.

Kết giao

Chọn lọc



Chú ý đề phòng

⚠ Những tài khoản để **tên và hình ảnh người ngoại quốc**, hoặc xưng Việt kiều kết bạn nhưng trước đó giữa bạn và họ không có bất kỳ mối liên kết nào (như bạn chung).

⚠ Những người dành nhiều lời có cánh, tha thiết **bày tỏ tình cảm dù mới quen**.

⚠ Thận trọng với những lời đề nghị tặng quà, tặng tiền... trên mạng. Nhưng dẫn dắt đến cuối cùng thì người phải bỏ tiền ra trước là ta.

⚠ **Đề phòng những doanh nhân, chuyên gia** xa lạ nào đó bỗng nhiên ngỏ lời muốn giúp đỡ bạn làm giàu...



3.

Kết giao

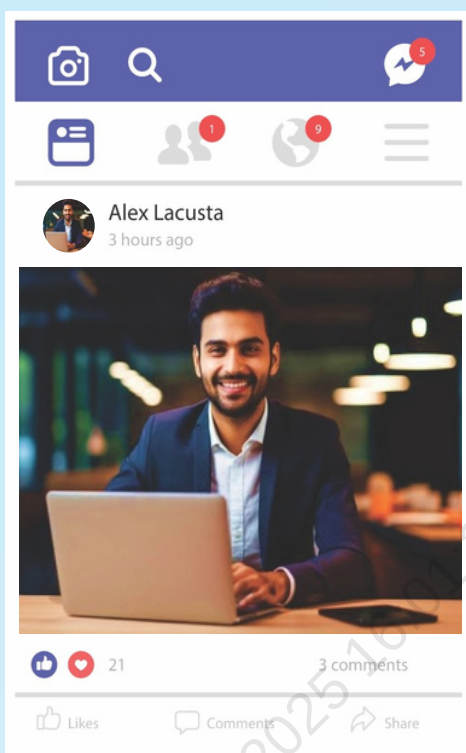
Chọn lọc 



Bạn có thấy người này đáng tin không?

Xin chào!!!

Xin chào! Xin hỏi bạn là ai?



Xin thứ lỗi cho tôi nếu làm bạn bất ngờ! Tôi tình cờ thấy hình ảnh của bạn và tôi thật sự rung động. Bạn vô cùng xinh đẹp trong mắt tôi và tôi không thể ngăn cản mong muốn bản thân tìm hiểu bạn. Bạn có phiền chút nào không?

Không phiền, nhưng tôi không biết bạn. Bạn là người nước nào?



Tôi tên Alex Lacusta, tôi sinh ra ở Trung Ấn nhưng hiện tại tôi là nhân viên của Google ở Mỹ. Tôi đã dùng công cụ dịch thuật Google dịch để nói chuyện với bạn. Hy vọng tôi không nói điều gì sai khi chuyển ngữ sang ngôn ngữ của bạn!



Hiện nay, hầu hết mạng xã hội đều có định vị quốc gia và gợi ý tìm kiếm kết bạn cùng quốc gia. Trường hợp người ở Việt Nam kết bạn được với những người ở quốc gia khác thường đã có quen biết từ trước, hoặc do bản thân chủ động tìm kiếm, kết nối.

* Góc tình huống

Alô! Xin hỏi Chị Xuân phải không ạ? Chào chị em là Mai, em đến từ trung tâm vận chuyển hàng không quốc tế DHL. Chị có một đơn hàng từ Mỹ gửi về. Em gọi để xác nhận. Thông tin đơn hàng là một chiếc nhẫn kim cương trị giá **16.800 USD** gửi từ anh David Lee. Do đơn hàng này giá trị cao, vận chuyển qua hải quan Việt Nam phải đóng thuế hàng xa xỉ là 5% giá trị hàng hoá. **Chị phải nộp phí** này cho hải quan mới được thông quan ạ.

LỪA ĐẢO



Chưa lấy được nhẫn đã bắt nộp tiền. Có tiền mua nhẫn nghìn đô lại không trả nổi phí thông quan. Tặng quà mà người được tặng phải tốn tiền? Bạn tin được không?



4.

Phòng tránh

Lừa đảo
trực tuyến



4.

Phòng tránh lừa đảo trực tuyến



Các hình thức lừa đảo trực tuyến phổ biến và cách phòng tránh

1. “Hack” (chiếm đoạt) Facebook, Zalo...



Chiếm quyền đăng nhập vào tài khoản hoặc Giả danh người trong video nhờ sử dụng công nghệ (deepfake) nhắn tin cho bạn bè người thân hỏi mượn tiền.

**Cách phòng tránh: Gọi vào số điện thoại hoặc gặp trực tiếp hỏi để chắc chắn. Tự bảo vệ tài khoản của mình bằng mật khẩu 2 lớp.*

2. Giả danh cơ quan pháp luật

Gọi điện, nhắn tin yêu cầu nạn nhân chuyển tiền vào số tài khoản do đối tượng cung cấp để phục vụ công tác điều tra.

**Cách phòng tránh: Theo quy định, cơ quan Nhà nước phải làm việc thông qua giấy mời, giấy triệu tập.*

4.

Phòng tránh lừa đảo trực tuyến



***Các hình thức lừa đảo trực tuyến phổ biến
và cách phòng tránh***



3. Các ứng dụng, hội, nhóm làm nhiệm vụ online kiếm tiền

Thủ đoạn chung là người tham gia phải nộp tiền, ban đầu sẽ được trả hoa hồng hoặc tiền lãi cao hơn số tiền bỏ ra. Sau đó lừa người tham gia nộp tiền nhiều hơn nhưng không thể rút lại nữa.

**Cách phòng tránh: Cần nhớ những hình thức kiếm nhiều tiền một cách dễ dàng, nhanh chóng, nếu không phải tội phạm thì là nạn nhân của tội phạm.*

4.

Phòng tránh lừa đảo trực tuyến



Các hình thức lừa đảo trực tuyến phổ biến và cách phòng tránh



4. Lấy cắp thông tin cá nhân Lừa đảo lấy cắp thông tin cá nhân, mật khẩu đăng nhập: bằng cách gửi các đường link lừa đảo, mã QR và phần mềm độc hại như quảng cáo, cảnh báo virus, bình chọn các cuộc thi cho người quen.

Cách phòng tránh: Không nhấn vào đường link hoặc quét mã QR đó nếu bản thân không chủ động tìm kiếm hoặc yêu cầu người khác gửi. **Hãy xem xét kỹ cấu trúc của đường link. Đừng nhập bất cứ thông tin gì vào trang web đó nếu chưa xác minh kỹ càng*

4.

Phòng tránh lừa đảo trực tuyến



Các hình thức lừa đảo trực tuyến phổ biến và cách phòng tránh

5. Đánh cắp thông tin Căn cước đi vay tín dụng

Sử dụng thông tin trên Căn cước bị hại, tin tặc đăng ký mã số thuế ảo, vay tiền từ các tổ chức tín dụng trên mạng xã hội và lừa đảo chiếm đoạt tài sản.



**Cách phòng tránh: Không chụp giấy tờ tùy thân đưa lên mạng, không cho người khác mượn giấy tờ tùy thân nếu không có lý do rõ ràng, phải giám sát khi cho người khác mượn, cân nhắc khi dùng giấy tờ tùy thân đăng ký thành viên trên những trang web, ứng dụng không đủ uy tín.*

4.

Phòng tránh lừa đảo trực tuyến



Các hình thức lừa đảo trực tuyến phổ biến và cách phòng tránh

6. Lừa đảo chuyển nhầm tiền

Đối tượng lừa đảo chuyển tiền vào tài khoản ngân hàng của nạn nhân: giả danh người thu hồi nợ để yêu cầu trả lại số tiền kèm lãi suất cao.

**Cách phòng tránh: Để nguyên hiện trạng, ra ngân hàng in sao kê và trình báo cơ quan công an.*



7. Lừa đảo “combo (trộn gói) du lịch giá rẻ”

Quảng cáo tour du lịch, phòng khách sạn giá rẻ để chiếm đoạt tiền đặt cọc hoặc lấy lý do thông tin kê khai không đầy đủ, chiếm đoạt tiền làm thủ tục visa.

**Cách phòng tránh: Chỉ đặt trên “App” (ứng dụng) du lịch và công ty du lịch uy tín.*

4.

Phòng tránh lừa đảo trực tuyến



Các hình thức lừa đảo trực tuyến mới và cách phòng tránh



8. Lừa đảo vé tàu, vé xe dịp Lễ, Tết

Lợi dụng thị trường tranh giành vé tàu, xe, lập các trang “Fanpage” (trạng mạng xã hội) giả mạo nhà xe đăng tin bán vé giá rẻ hơn thị trường để lừa người mua chuyển tiền sau đó chặn liên lạc.

**Cách phòng tránh: Chỉ đặt trên các ứng dụng và trang web chính thống. Không tin tưởng chuyển tiền cho bất kỳ cá nhân nào.*

4.

Phòng tránh lừa đảo trực tuyến



Các hình thức lừa đảo trực tuyến mới và cách phòng tránh



9. Lừa đảo bằng cách đăng khuyến cáo các thủ đoạn lừa đảo

Đăng thông tin khuyến cáo các thủ đoạn lừa đảo trực tuyến và biện pháp phòng ngừa để lợi dụng lòng tin của nạn nhân muốn nhanh chóng lấy lại tài khoản, sẵn sàng chi tiền mua dịch vụ lấy lại tài khoản.

**Cách phòng tránh: Đừng tin tưởng đưa tiền cho người khác trước khi nhận được kết quả. Mỗi nền tảng mạng xã hội, hay ứng dụng đều có hướng dẫn của nhà cung cấp dịch vụ về cách khôi phục tài khoản.*

4.

Phòng tránh lừa đảo trực tuyến



Lời khuyên cho bạn



- Tiền còn trong tay mình là tiền chủ động, rơi vào tay người khác là tiền bị động. Hãy **chậm lại vài giây** trước khi đưa ra bất kỳ quyết định tài chính nào.
- Tài khoản trực tuyến chứa đựng nhiều thông tin, hoạt động cá nhân. Phải **xem xét kỹ** trước khi nhập thông tin đăng nhập vào bất cứ đâu trên không gian mạng.

* Góc tình huống

Cuộc trò chuyện bất ổn! Người thân gọi video call mượn tiền nhưng:

- Khuôn mặt trong cuộc gọi không tự nhiên, không rõ nét;
- Âm thanh không đồng nhất với clip, nhiều tiếng ồn, âm thanh ngắt quãng hoặc tắt tiếng;
- Bị ngắt giữa chừng, người gọi bảo là sóng yếu.

Nên ✓



Giả vờ hỏi người thân một nội dung nào đó mà biết chắc nếu người khác giả mạo sẽ trả lời sai để kiểm tra.

Liên lạc trực tiếp với người thân, bạn bè thông qua một kênh khác xem có đúng là họ cần tiền không?



**Hãy cùng chia sẻ các nội
dung hữu ích với gia đình
và bạn bè để giúp người
dân Việt Nam an toàn hơn
trên Internet!**





congan.danang.gov.vn

**Facebook, Zalo của Phòng An ninh mạng
và phòng, chống tội phạm sử dụng công nghệ cao,
Công an thành phố Đà Nẵng**

facebook



Zalo



**PHÒNG AN NINH MẠNG VÀ PCTP SỬ DỤNG CÔNG NGHỆ CAO
- CÔNG AN THÀNH PHỐ ĐÀ NẴNG**