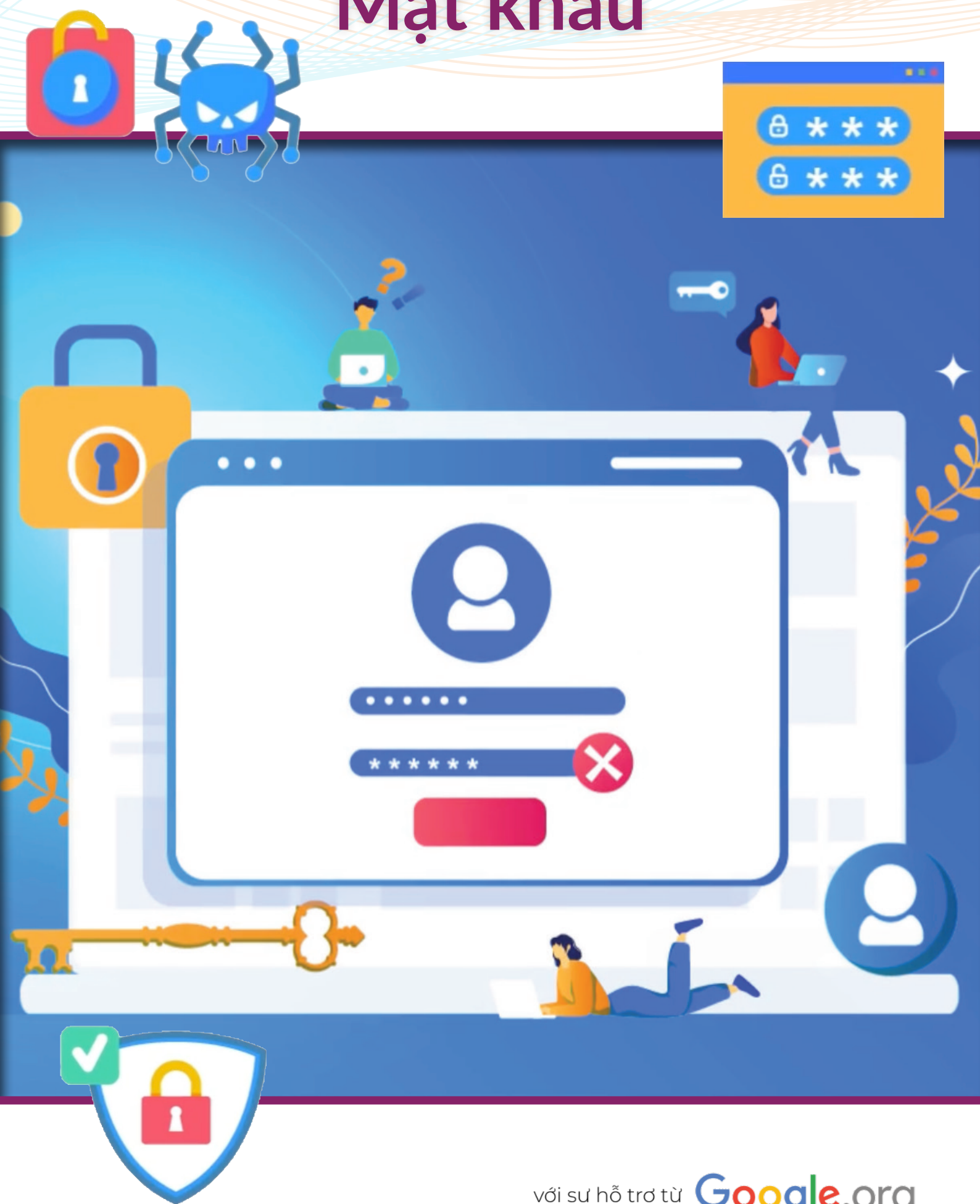


CHỦ ĐỀ 2: BẢO VỆ THÔNG TIN VÀ CÁC TÀI KHOẢN TRỰC TUYẾN

Bài 1: Mật khẩu



MỤC TIÊU:

- Hiểu biết cơ bản về mật khẩu và tầm quan trọng của mật khẩu
- Biết đặt mật khẩu mạnh và các thực hành khiến mật khẩu yếu đi
- Hiểu và thực hành về việc xác thực hai (đa) yếu tố



Mật khẩu đóng vai trò vô cùng quan trọng trong việc bảo vệ thông tin cá nhân và tài khoản trực tuyến. Chúng ta sử dụng mật khẩu để bảo vệ tài khoản ngân hàng, thư điện tử, mạng xã hội và nhiều dịch vụ trực tuyến khác. Tuy nhiên, việc tạo và quản lý mật khẩu không phải lúc nào cũng dễ dàng nếu không thực sự hiểu và thực hành đúng cách.

1. Mật khẩu và tầm quan trọng của mật khẩu



Hãy xem xét ví dụ sau: Anh Hòa sử dụng tài khoản Facebook cá nhân để kinh doanh nông sản sạch, nơi anh thường xuyên đăng bài giới thiệu sản phẩm, livestream bán hàng và giao tiếp với hơn 5.000 bạn bè.

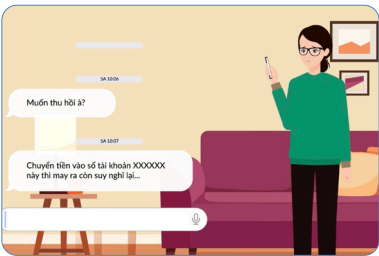
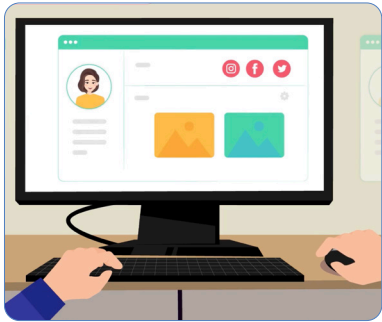
Đây là kênh bán hàng chính mang lại thu nhập ổn định mỗi tháng. Một ngày, anh nhận được tin nhắn từ một tài khoản lạ mời hợp tác làm đối tác phân phối nông sản trên một sàn thương mại điện tử. Tin nhắn đính kèm một đường link đăng ký “trông có vẻ chuyên nghiệp”. Tin tưởng, anh Hòa nhấn vào và đăng nhập bằng tài khoản Facebook. Chỉ vài phút sau, anh bị đăng xuất khỏi tài khoản. Tài khoản bị kẻ xấu chiếm đoạt, đăng bán hàng kém chất lượng, gây ảnh hưởng nghiêm trọng đến uy tín và khiến nhiều khách hàng hiểu lầm. Trong khi đó, việc kinh doanh của anh Hòa cũng bị gián đoạn và anh bị mất rất nhiều khách quen.

Trên thực tế, khi tham gia “ngôi làng số”, chúng ta có rất nhiều các tài khoản trực tuyến. Tài khoản trực tuyến là tài khoản lưu trữ thông tin cá nhân và tài chính quan trọng của mỗi cá nhân hay tổ chức. Mỗi tài khoản được ví như một ngôi nhà, và mật khẩu của bạn có thể được ví như ổ khóa hay chìa khóa để vào ngôi nhà. Và nếu chúng ta sử dụng một ổ khóa với chìa khóa lỏng lẻo và dễ dàng bị phá bỏ thì kẻ trộm sẽ có nhiều cơ hội để đột nhập vào căn nhà. Cũng như vậy, nếu dùng một mật khẩu yếu sẽ khiến cho tài khoản của bạn dễ dàng bị đánh cắp. Khi kẻ xấu “đột nhập” vào “căn nhà tài khoản” của bạn, chúng sẽ có thể tiếp cận được các tài sản số và gây ra các rủi ro số. Những rủi ro anh Hòa gặp phải ở trên chỉ là một trong số các rủi ro số mà bạn có thể gặp phải nếu không bảo mật tài khoản trực tuyến của mình. Tổng hợp lại sau đây là một vài rủi ro số chính mà bạn nên cảnh giác:



Rủi ro liên quan đến thông tin cá nhân: Kẻ xấu có thể truy cập và sử dụng thông tin của bạn như họ tên, ngày sinh, địa chỉ, số điện thoại... để mạo danh hoặc thực hiện các hành vi gian lận, lừa đảo.

Rủi ro liên quan đến danh sách bạn bè: Bạn bè trong danh sách của bạn có thể trở thành mục tiêu bị lừa đảo, chẳng hạn như bị kẻ xấu mạo danh yêu cầu chuyển tiền hoặc cung cấp thông tin nhạy cảm.



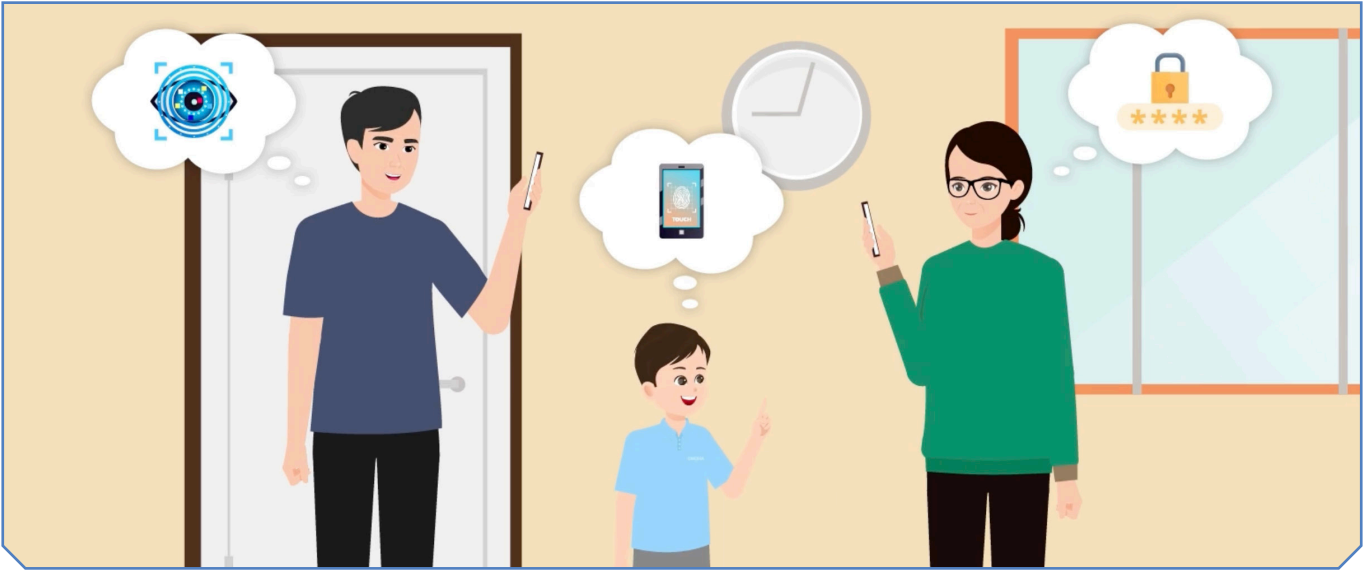
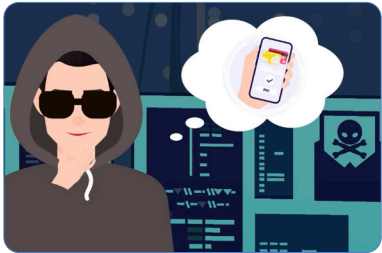
Rủi ro liên quan đến dữ liệu cá nhân: Các hình ảnh, video, và tin nhắn riêng tư của bạn có thể bị kẻ xấu phát tán công khai hoặc sử dụng để đe dọa, tống tiền.

Rủi ro liên quan đến danh tính và danh tiếng: Kẻ xấu có thể đăng nội dung không phù hợp lên tài khoản của bạn, gây tổn hại đến danh tiếng cá nhân, đặc biệt là với người nổi tiếng hoặc người kinh doanh trên nền tảng trực tuyến.



Rủi ro liên quan đến tài chính: Nếu tài khoản trực tuyến của bạn liên kết với tài khoản ngân hàng hoặc ví điện tử, kẻ xấu có thể từ đó đánh cắp tiền từ các tài khoản này của bạn. Trong trường hợp kinh doanh, dữ liệu khách hàng hoặc các giao dịch quan trọng của bạn cũng có nguy cơ bị đánh cắp.

Rủi ro liên quan đến các mối quan hệ: Kẻ xấu có thể mạo danh bạn, làm ảnh hưởng xấu tới mối quan hệ của bạn với người thân, bạn bè, đồng nghiệp.



Vì vậy, việc sở hữu một mật khẩu mạnh sẽ giúp bạn bảo vệ các tài sản số, tránh được các rủi ro, giữ gìn những giá trị quý giá trong cuộc sống số. Quan tâm tới việc bảo mật mật khẩu chính là cách bạn bảo vệ chính mình và những người xung quanh trước những rủi ro số.

2. Thế nào là một mật khẩu mạnh?

Để bảo vệ tài khoản và mật khẩu, việc đặt mật khẩu mạnh cho tài khoản là một điều cần thiết. Vậy thế nào là một mật khẩu mạnh và làm thế nào để chúng ta có thể tạo ra một mật khẩu mạnh? Trước tiên, hãy cùng xem xét bảng thống kê sau đây:

HẠNG	MẬT KHẨU	THỜI GIAN ĐỂ PHÁ
1	123456	< 1 giây
2	123456789	< 1 giây
3	anhyeuem	< 1 giây
4	123456789	< 1 giây
5	password	< 1 giây
6	maiyeuem	3 giờ
7	12345678	< 1 giây
8	1234567	< 1 giây
9	khongbiet	1 ngày
10	123123	< 1 giây

Hình 2.1. Top 10 mật khẩu dễ đoán nhất ở Việt Nam (Nguồn: NordPass, 2022)

NordPass đã thống kê top 10 mật khẩu thông dụng nhất năm 2022 tại Việt Nam như “123456”, “123456789”, “anhyeuem” (Hình 2.1). Cũng theo NordPass, Việt Nam thuộc trong top 5 quốc gia Đông Nam Á sử dụng mật khẩu dễ đoán nhất. Giống như một ổ khóa lỏng lẻo dễ bị phá, các mật khẩu dễ đoán này mặc dù dễ nhớ nhưng lại tạo điều kiện thuận lợi cho kẻ xấu có thể dễ dàng xâm nhập. Thời gian để phá các mật khẩu này có thể tính bằng giây, nhiều nhất là 1 ngày. Do đó, chúng ta nên tránh đặt các mật khẩu thông dụng và dễ đoán.

Một mật khẩu mạnh giúp chúng ta có thể bảo vệ thông tin và nhiều tài sản số liên quan. Mặc dù mật khẩu mạnh không hoàn toàn đảm bảo các tài khoản không bao giờ bị chiếm đoạt (hack), nhưng nó sẽ tăng khả năng bảo vệ tài khoản của chúng ta hơn. Mật khẩu mạnh là mật khẩu đảm bảo các yếu tố sau:

Tối thiểu 8-12 ký tự

Gồm chữ hoa

ABC

Và chữ thường

abc

Có ít nhất một số

123

Một kí hiệu đặc biệt

@#&

#T0iy3uHanoi

Bạn cần lưu ý, **độ dài của mật khẩu** là bí quyết cho một công thức mật khẩu mạnh. Mật khẩu càng dài thì thời gian để có thể phá khóa càng lâu. Hãy thử tham khảo cách sau:

- **Sử dụng một chuỗi gồm nhiều từ riêng biệt để tạo mật khẩu.** Để dễ ghi nhớ, bạn nên chọn các từ có mối liên kết chung hoặc các thông tin liên quan đến bạn nhưng ít người biết.
Ví dụ: *kem + táo + bánh + Hà Nội* sẽ tạo thành mật khẩu: *kemtaobanhHanoi*. Trong đó kem, táo, bánh là 3 đồ ăn bạn thích nhất và Hà Nội là nơi bạn sinh ra.
- Để tăng độ khó cho mật khẩu, bạn có thể biến các ký tự chữ và số thành các ký tự đặc biệt.

Ví dụ: Chữ “e” thành số “3”, chữ “a” thành “@”, khi đó bạn sẽ có mật khẩu “k3mt@ob@nhH@noi”.

- Ngoài ra, bạn cũng có thể sử dụng chữ cái đầu của tên một bài hát, bộ phim yêu thích hoặc một câu nói quen thuộc để tạo ra một mật khẩu đủ dài nhưng vẫn dễ nhớ. Ví dụ, nếu bạn rất thích bài hát “Năm anh em trên một chiếc xe tăng”, bạn có thể tạo mật khẩu là 5Aetmcxt!

SUY NGẪM

Mật khẩu nào là mật khẩu mạnh nhất trong số các mật khẩu sau?

- A. ToiYeuHaNoi@2023
- B. Abc123
- C. 66668888
- D. Xyz2025

(Đáp án: A vì có đủ độ dài, bao gồm chữ hoa, chữ thường, số và ký tự đặc biệt nên đạt yêu cầu của một mật khẩu mạnh. Các lựa chọn khác dễ đoán hoặc quá đơn giản.)

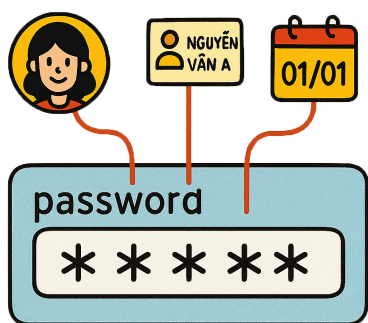
3. Điều gì khiến mật khẩu yếu đi?

Việc tạo ra một mật khẩu mạnh là bước đầu tiên trong việc bảo vệ tài khoản của bạn. Tuy nhiên, ngay cả khi bạn tạo một mật khẩu thực sự khó đoán đối với máy tính hay người muốn bẻ khóa (hacker) thì có những thực hành có thể khiến cho mật khẩu của bạn suy yếu đi như:



Sử dụng một mật khẩu cho nhiều tài khoản:

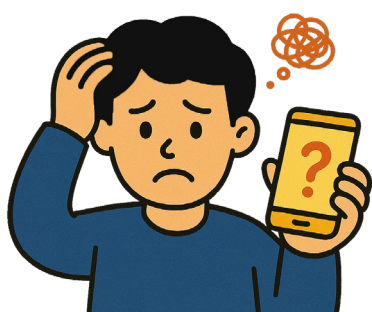
Nếu một tài khoản của bạn bị xâm nhập, tất cả các tài khoản khác cũng sẽ bị nguy hiểm. Điều này làm tăng rủi ro mất thông tin cá nhân và tài sản số của bạn. Hơn nữa, hacker có thể dễ dàng truy cập vào nhiều dịch vụ và gây ra thiệt hại lớn hơn.



Sử dụng mật khẩu chứa thông tin cá nhân: Hacker có thể dễ dàng đoán được mật khẩu của bạn do các thông tin như tên, ngày sinh, hoặc số điện thoại rất dễ bị lộ và bị khai thác.

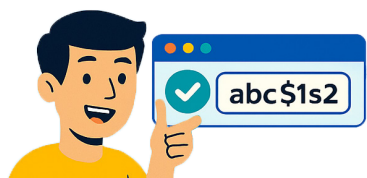


Sử dụng cùng một mật khẩu trong thời gian dài: Mật khẩu cũ có thể bị lộ qua thời gian và trở nên dễ đoán hơn. Các hacker thường xuyên tìm kiếm và khai thác các mật khẩu đã bị lộ từ các vụ rò rỉ dữ liệu trước đó. Ngoài ra, công nghệ và phương pháp tấn công của hacker ngày càng tinh vi, nên mật khẩu cũ có thể không còn đủ mạnh để bảo vệ tài khoản của bạn.



Quên mật khẩu: Dù chúng ta đặt mật khẩu an toàn đến đâu thì một khi quên mật khẩu thì mọi chuyện đều trở nên vô nghĩa. Khi đó, chúng ta sẽ mất thời gian để có thể lấy lại mật khẩu. Thậm chí, nếu không còn nhớ các thông tin để có thể lấy lại mật khẩu thì chúng ta còn đối mặt với rủi ro mất luôn tài khoản đó.

Bởi vậy, để giúp cho mật khẩu của chúng ta tránh các rủi ro, chúng ta cần phải lưu ý các thực hành sau:



Mật khẩu có thể khó đoán nhưng nên dễ nhớ.



Trong trường hợp có nhiều mật khẩu phức tạp và khó nhớ, bạn có thể sử dụng trình quản lý mật khẩu. Trình quản lý mật khẩu là một trang web/ứng dụng để người dùng lưu và sắp xếp mật khẩu của mình.



Mật khẩu không nên là một từ thông dụng hoặc chứa thông tin cá nhân (ngày sinh, tên cha mẹ, con cái v.v).



Không nên dùng chung mật khẩu cho nhiều ứng dụng, trang web dịch vụ.



Thay đổi mật khẩu định kỳ ít nhất từ 3-6 tháng.



Không nên chia sẻ mật khẩu cá nhân với người khác và luôn cảnh giác với những yêu cầu cung cấp mật khẩu tài khoản.

4. Xác thực hai (đa) yếu tố

Để tăng cường an ninh cho một ngôi nhà, đôi khi chúng ta sử dụng nhiều lớp cửa với nhiều ổ khóa và chìa khóa. Tương tự như vậy, bạn cũng có thể sử dụng nhiều lớp bảo vệ thay vì chỉ sử dụng mật khẩu. Khi đó, bạn sử dụng **xác thực hai yếu tố** (2FA: two-factor authentication) hoặc **đa yếu tố** (MFA: multi-factor authentication). Các biện pháp này yêu cầu người dùng cung cấp nhiều hơn một yếu tố để xác minh danh tính khi đăng nhập hoặc thực hiện các hành động trên một tài khoản (ví dụ: thay đổi mật khẩu, thay đổi email liên kết với tài khoản, thay đổi thông tin thanh toán...). Xác thực hai yếu tố yêu cầu hai thông tin riêng biệt trước khi cấp cho bạn quyền truy cập tài khoản hoặc thực hiện các hành động này.

Cách hoạt động thường thấy của xác thực đa yếu tố hay 2 yếu tố là khi bạn đăng nhập tài khoản trên một thiết bị lần đầu tiên thì hệ thống sẽ yêu cầu bạn nhập mật khẩu (yếu tố đầu tiên), sau đó hỏi bạn 1 thông tin khác được cập nhật qua một thiết bị khác (yếu tố thứ hai), ví dụ: mã xác minh được gửi qua tin nhắn điện thoại. Chỉ khi bạn nhập thành công yếu tố thứ hai này thì bạn mới có thể đăng nhập được vào tài khoản. Do đó, phương pháp này có thể giúp tài khoản của bạn an toàn hơn nhiều bằng cách thêm một lớp bảo mật bổ sung khó bị phá vỡ hơn.

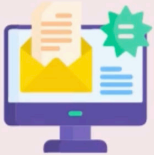


Yếu tố trong xác thực là một cách xác nhận danh tính của bạn khi bạn cố gắng đăng nhập. Các yếu tố này có thể được chia làm ba loại:

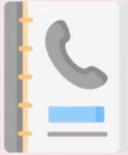
YẾU TỐ BẠN CÓ



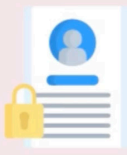
Điện thoại



Thư điện tử



Số điện thoại



Tài khoản

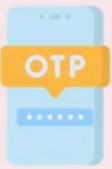
YẾU TỐ BẠN BIẾT



Mật khẩu



Mã PIN



Mã xác minh

YẾU TỐ BẠN SỞ HỮU



Vân tay

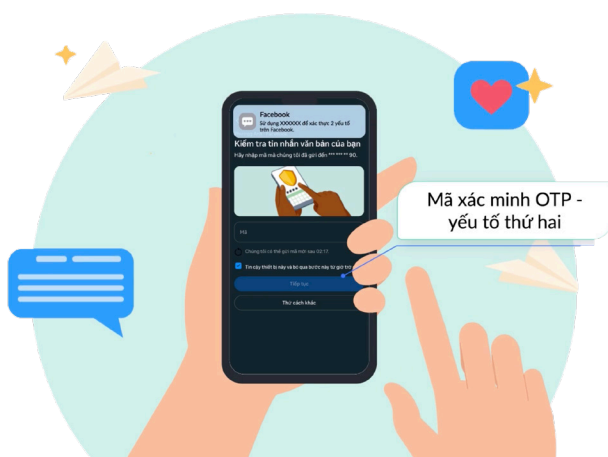


Nhận dạng khuôn mặt

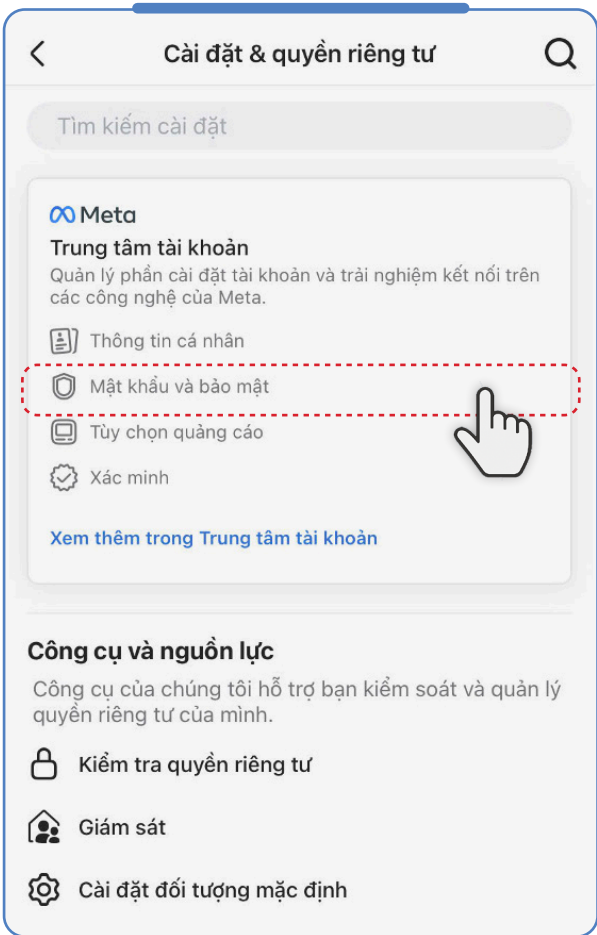
Thông thường, ngoài việc yêu cầu mật khẩu, người dùng thường lựa chọn phương án nhập **mã xác minh một lần - OTP** (được gửi qua tin nhắn văn bản, ứng dụng hoặc email), và mã này phải được nhập ngay sau khi nhập mật khẩu. Khi đó, để đăng nhập vào tài khoản của bạn, một người phải có mật khẩu của bạn và họ cần có cả quyền truy cập vào ứng dụng, thiết bị hoặc địa chỉ email được liên kết với tài khoản của bạn để nhận mã xác minh một lần. Do đó, việc bật xác thực 2 yếu tố trên các ứng dụng, nền tảng hay trang web chứa tài khoản của bạn là một bước rất quan trọng trong việc bảo vệ tài khoản của bạn.

Hãy xem xét ví dụ sau: Chị Lan muốn đăng nhập vào tài khoản Facebook trên một thiết bị mới. Vì tài khoản đã bật xác thực hai yếu tố, hệ thống sẽ yêu cầu chị nhập mật khẩu trước. Sau khi nhập đúng mật khẩu, Facebook tiếp tục gửi một mã xác minh OTP đến số điện thoại đã đăng ký của chị. Chỉ khi nhập đúng mã này, chị mới có thể đăng nhập thành công. Như vậy, nếu ai đó muốn truy cập vào tài khoản của chị Lan, họ không chỉ cần biết mật khẩu mà còn phải có quyền truy cập vào tin nhắn chứa mã OTP trên điện thoại của chị. Nếu chị Lan không để người khác tiếp cận điện thoại, cũng như không gửi mã OTP cho bất kỳ ai thì nguy cơ chị bị chiếm đoạt tài khoản sẽ thấp hơn nhiều so với khi không bật tính năng xác thực hai yếu tố.

Để bật xác thực đa yếu tố cho các tài khoản trực tuyến của mình, thông thường bạn hãy truy cập vào **Cài đặt**, tìm mục **Bảo mật/ Cài đặt bảo mật**, sau đó tìm tùy chọn **Xác thực hai (đa) yếu tố** và bật tùy chọn này sau đó làm theo các hướng dẫn. Lưu ý rằng đôi khi các hệ thống sẽ yêu cầu bạn nhập mật khẩu một lần nữa trước khi bật tính năng này, do đó việc ghi nhớ mật khẩu của tài khoản là vô cùng quan trọng.

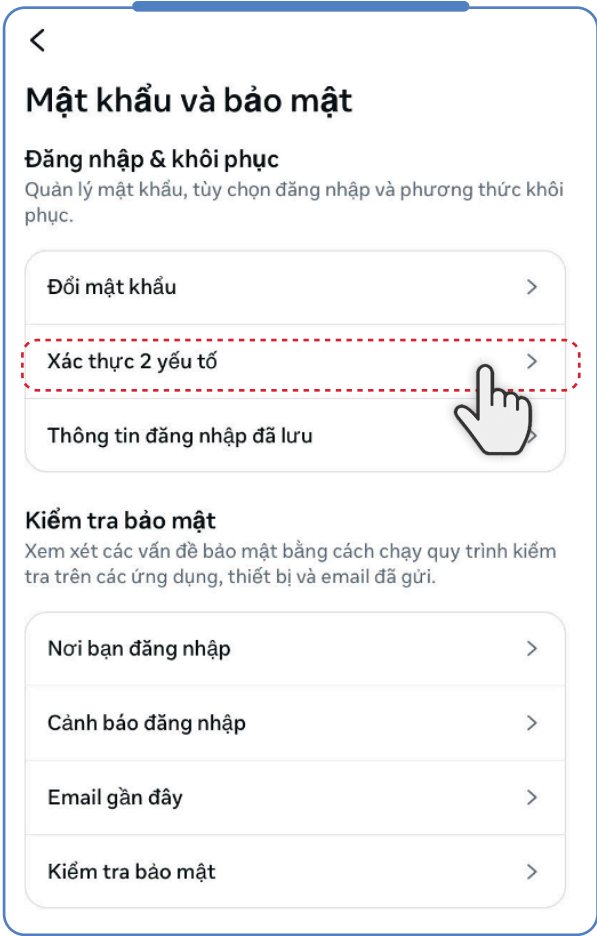
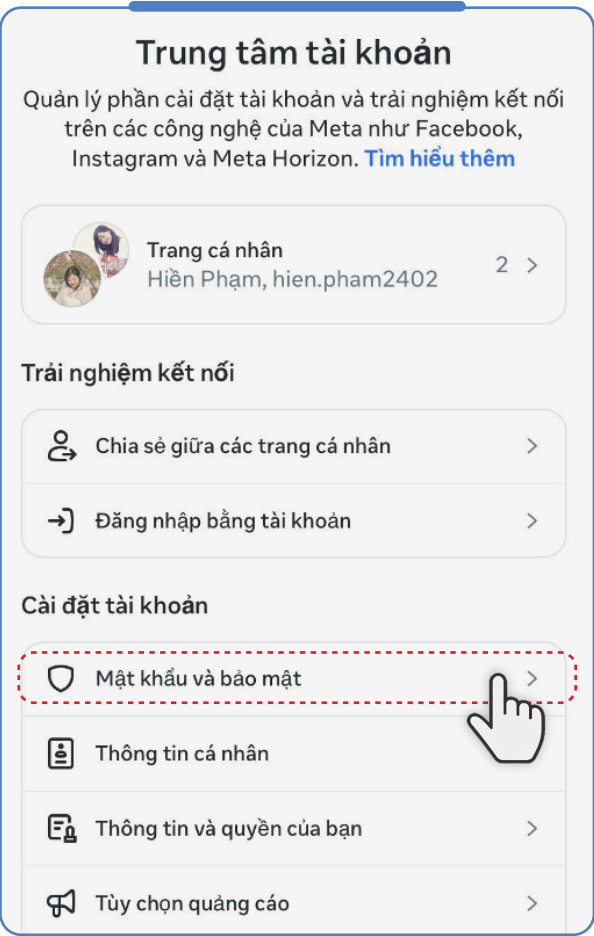


Dưới đây, bạn có thể tham khảo các bước bật Xác thực hai yếu tố trên nền tảng Facebook:



BƯỚC 1: Vào Menu, bấm chọn **Cài đặt & quyền riêng tư**, sau đó bấm **Cài đặt**

BƯỚC 2: Bấm chọn **Mật khẩu và bảo mật**

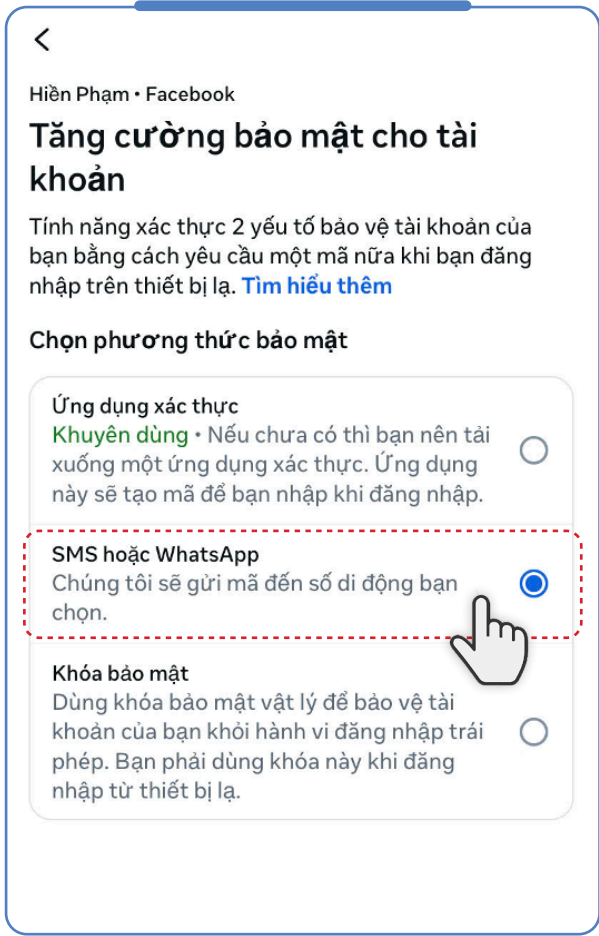


BƯỚC 3: Bấm chọn **Mật khẩu và bảo mật**

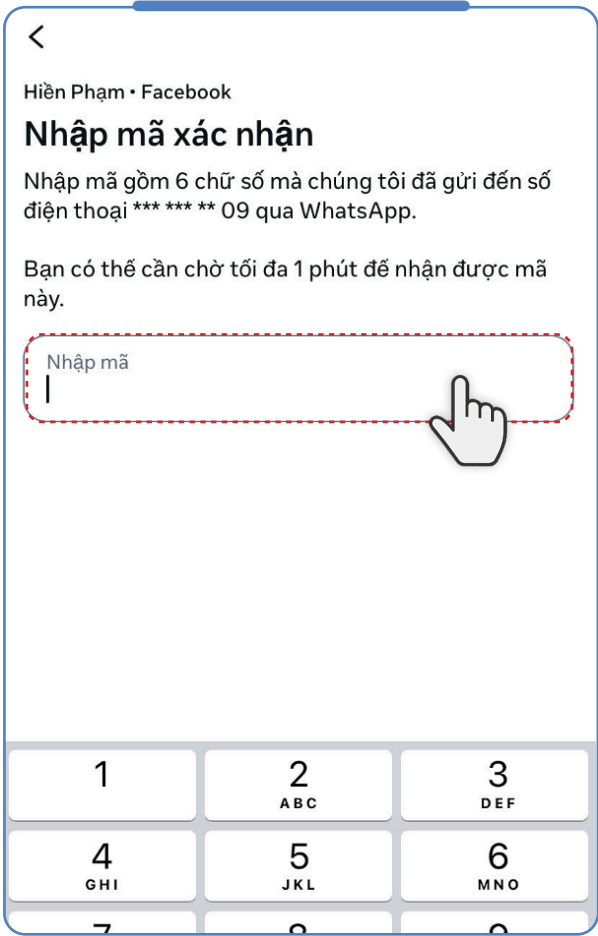
BƯỚC 4: Bấm chọn **Xác thực 2 yếu tố**



BƯỚC 5: Nhập lại mật khẩu tài khoản



BƯỚC 6: Chọn phương thức nhận yếu tố thứ 2, ví dụ **SMS** hoặc **WhatsApp**



BƯỚC 7: Nhập mã xác nhận gửi về số điện thoại đăng ký



BƯỚC 8: Bấm vào **Xong** để hoàn tất

Nội dung chính cần ghi nhớ

1. Mật khẩu giống như ổ khóa hoặc chìa khóa vào ngôi nhà của bạn. Việc dùng mật khẩu yếu sẽ khiến cho tài khoản của bạn dễ dàng bị đánh cắp và đối mặt với rủi ro đánh mất thông tin, danh tính, tiền hay các mối quan hệ.

2. Mật khẩu mạnh là mật khẩu đảm bảo các yếu tố sau:

- Mật khẩu nên có tối thiểu 8-12 ký tự.
- Bao gồm ít nhất một số.
- Bao gồm ít nhất một ký hiệu.
- Bao gồm ít nhất một chữ viết hoa và một chữ viết thường.

Lưu ý độ dài mật khẩu có thể sẽ góp phần quyết định độ an toàn của mật khẩu đó.

3. Để mật khẩu của bạn không suy yếu đi, hãy lưu ý:

- Mật khẩu có thể khó đoán nhưng nên dễ nhớ (trừ khi sử dụng trình quản lý mật khẩu).
- Sử dụng trình quản lý mật khẩu - đó là một trang web/ứng dụng để người dùng lưu và sắp xếp mật khẩu của mình.
- Mật khẩu không nên là một từ thông dụng hoặc chứa thông tin cá nhân (ngày sinh, tên cha mẹ, v.v).
- Không nên dùng chung mật khẩu giữa nhiều trang web, ứng dụng.
- Thay đổi mật khẩu định kỳ ít nhất từ 3-6 tháng.

4. Xác thực hai yếu tố hoặc đa yếu tố là một biện pháp bảo mật bổ sung, yêu cầu người dùng cung cấp nhiều hơn một yếu tố để xác minh danh tính khi đăng nhập hoặc thực hiện một hành động trên một tài khoản. Đây cũng là bước cần thiết quan trọng không thể thiếu để bảo vệ tài khoản của bạn không bị xâm nhập khi kẻ xấu đã đoán hoặc phá được mật khẩu.