Mật khẩu

Học viên sẽ học cách giữ cho thông tin trên mạng của họ an toàn hơn qua việc sử dụng và duy trì các mật khẩu mạnh. Ngoài ra, học viên sẽ tìm hiểu về các nguyên tắc tạo mật khẩu mạnh, các vấn đề tiềm ẩn khi chia sẻ mật khẩu. Họ cũng sẽ tìm hiểu cách bảo vệ mật khẩu và các bước ngăn chặn hành vi truy cập trái phép vào tài khoản của mình.

Tài liệu

- Phiếu bài tập Tìm hiểu về mật khẩu

Thông tin cơ bản về mật khẩu

Phần 1

Nói với học viên

Chúng ta thường không nghĩ nhiều về những mật khẩu mà mình dùng cho các trang web, ứng dụng và dịch vụ. Tuy nhiên, độ mạnh của mật khẩu sẽ quyết định mức độ an toàn của thông tin.

Tương tác trong lớp

Hãy dùng các câu hỏi sau để khơi gợi cho cả nhóm cùng thảo luận. Nhắc học viên nhớ rằng không được chia sẻ mật khẩu thực sự của mình trong bài tập này hoặc bất kỳ bài tập nào khác.

Hỏi học viên

Mỗi người chúng ta có bao nhiêu mật khẩu?

> Chúng ta có các mật khẩu khác nhau cho mỗi tài khoản email và tài khoản mạng xã hội không?
>
> Các mật khẩu đó hoàn toàn khác nhau hay chỉ là biến thể của một mật khẩu?

Nếu có nhiều mật khẩu, làm thế nào để chúng ta nhớ được mật khẩu nào thuộc tài khoản nào?

Hỏi học viên

Chúng ta có thường xuyên quên mật khẩu quan trọng không?

> Chúng ta đã làm gì khi quên mật khẩu?
>
> Làm cách nào để mật khẩu của chúng ta dễ nhớ?

Chúng ta có sử dụng mật khẩu nào hàng ngày không?

Điều gì sẽ xảy ra nếu ai đó có được mật khẩu mà chúng ta không hề hay biết?

> Tình huống này có tùy xem người đó là ai không?

Một người có thể thu thập loại thông tin nào về chúng ta nếu họ dùng mật khẩu có

được để đăng nhập vào tài khoản của chúng ta?

Phần 2

Tương tác trong lớp

Chia học viên thành các cặp.

Nói với học viên

Thảo luận với người còn lại trong cặp về hậu quả có thể xảy ra, nếu một người có dụng ý xấu biết mật khẩu truy cập vào nền tảng mạng xã hội mà chúng ta yêu thích.

Tương tác trong lớp

Học viên có 5 phút để thảo luận. Sau đó, yêu cầu các nhóm chia sẻ ý kiến.

Nói với học viên

Bây giờ, hãy thảo luận theo cặp về hậu quả sẽ xảy ra nếu tin tặc biết được mật khẩu tài khoản ngân hàng trực tuyến của cha mẹ/người chăm sóc mình.

Tương tác trong lớp

Học viên có 5 phút để thảo luận. Sau đó, yêu cầu các nhóm chia sẻ những gì họ đã thảo luận.

Phần 3

Nói với học viên

Có thể chúng ta đang tự hỏi làm sao tin tặc lại biết được mật khẩu cá nhân. Có vài cách; một trong số đó là sử dụng kỹ thuật lừa đảo qua mạng (social engineering) hay dẫn dụ ai đó chia sẻ mật khẩu của họ. Tin tặc có thể làm vậy bằng cách gửi một email trông như thật sự đến từ nền tảng hay trang web mà một người có tài khoản. Email này có thể yêu cầu người đó nhấp vào một liên kết, rồi đăng nhập bằng tên người dùng và mật khẩu của họ; khi họ làm vậy thì thông tin này sẽ rơi vào tay tin tặc.

Đôi khi, tin tặc cố đoán mật khẩu bằng cách sử dụng các cụm từ thông dụng như “password123,” “test” hoặc họ tên của chúng ta.

Một cách khác để tin tặc biết được mật khẩu cá nhân là sử dụng kỹ thuật dò mật khẩu (Brute Force). Kỹ thuật dò mật khẩu sẽ được dùng khi tin tặc cố đăng nhập vào tài khoản của chúng ta bằng cách thử đi thử lại nhiều mật khẩu khác nhau. Dù có thể làm theo cách thủ công, nhưng kỹ thuật này thường được tiến hành bằng cách chạy

một chương trình máy tính tự động, dùng thử mọi cách kết hợp mật khẩu khả dĩ mà chương trình này nghĩ ra ở tốc độ cao. Ví dụ: một danh sách gồm các mật khẩu dễ đoán hoặc một loạt mật khẩu bao gồm các tổ hợp chữ cái và số khác nhau, cho đến khi họ tìm ra đúng thì thôi.

Đương nhiên, một số kỹ thuật dò mật khẩu có thể tinh vi hơn. Nếu mật khẩu của chúng ta nằm trong danh sách dễ đoán, chẳng hạn như “fido123” hoặc “password”, thì một số chương trình có thể đoán ra nhanh hơn bằng cách thử các lựa chọn này trước, rồi mới đến những mật khẩu ít khả năng hơn hoặc các mật khẩu được tạo ngẫu nhiên. Kỹ thuật tấn công này lại càng hiệu quả hơn nếu tin tặc biết thông tin về chúng ta. Ví dụ: nếu biết tên thú cưng của chúng ta là Toby, tin tặc có thể thử kết hợp từ "Toby" với biến thể của các số khác nhau ở cuối (chẳng hạn như "Toby629" hay "Toby3020").

Nguyên tắc tạo mật khẩu

Phần 1

Hỏi học viên

Có ai hiểu ý nghĩa của việc có một mật khẩu “mạnh” hoặc “cực mạnh” không? Tại sao nên có một mật khẩu như vậy?

Nói với học viên

Nhờ mật khẩu mạnh, chúng ta có thể bảo vệ thông tin của mình. Mặc dù có mật khẩu mạnh cũng không đảm bảo tài khoản của chúng ta sẽ chẳng bao giờ bị hack, nhưng mật khẩu yếu sẽ tạo cơ hội cho người khác dễ dàng truy cập thông tin của chúng ta hơn.

Bài tập về mật khẩu

Hỏi học viên

Hãy nêu một số ví dụ về mật khẩu yếu?

1. Có thể là: Password, 12345, Hello!, ngày sinh, biệt danh.

Vì sao chúng ta nghĩ đây là những mật khẩu yếu?

1. Người khác và/hoặc một chương trình máy tính chạy kỹ thuật dò mật khẩu có thể dễ dàng đoán ra những mật khẩu này.

Vậy có những cách nào để mật khẩu được kiên cố hơn?

1. Thêm các con số, chữ viết hoa và chữ viết thường, ký hiệu, tạo mật khẩu dài hơn và tránh các từ cũng như cụm từ thông dụng.

Tương tác trong lớp

Khi học viên đóng góp ý kiến xong, hãy viết những hướng dẫn sau lên bảng:

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.

Mật khẩu nên có tối thiểu 7 ký tự.

Mật khẩu nên dễ nhớ (trừ khi 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, v.v).

Không nên dùng chung mật khẩu giữa nhiều trang web.

Nói với học viên

Có hai phương pháp tạo mật khẩu mạnh. Một là làm như “công thức tạo mật khẩu” giống như trên bảng. Theo đó, một mật khẩu chỉ toàn chữ/số thông thường sẽ có thêm các thành phần khó đoán hơn, nhờ vậy mà không bị suy ra dễ dàng. Nhưng cũng vì thế mà nhược điểm của phương pháp này là mật khẩu trở nên khó nhớ hơn.

Mật khẩu mạnh

Nói với học viên

Một phương pháp khác để tạo mật khẩu mạnh đó là lưu ý đến độ dài của mật khẩu. Do độ mạnh của mật khẩu liên quan đến độ dài của mật khẩu, nên khi dùng một chuỗi gồm 4 từ không liên quan trở lên sẽ khiến người khác và các kỹ thuật dò mật khẩu gặp nhiều khó khăn. Phương pháp này còn có thêm một lợi ích nữa, đó là mật khẩu dễ nhớ hơn so với cách dùng công thức.

Cuối cùng, một người có thể kết hợp cả hai phương pháp này bằng cách tạo một chuỗi gồm 4 từ không liên quan trở lên, kèm theo các ký hiệu và số.

Những phương pháp khác nhau này đều có chung mục tiêu, đó là tạo ra những mật khẩu độc nhất mà người khác khó đoán được.

Nói với học viên

Chia học viên thành từng cặp.

Mỗi cặp sẽ cố gắng tạo ra một mật khẩu mạnh bằng cách làm theo các hướng dẫn đã viết trên bảng. Hãy nhớ rằng một mật khẩu mà máy tính khó đoán một cách ngẫu nhiên vẫn có thể dễ đoán nếu người khác hoặc máy tính có danh sách các mật khẩu dài thông dụng. Tờ giấy ghi mật khẩu của chúng ta sẽ không bị thu lại khi hoạt động này kết thúc. Tuy nhiên, chúng ta không nên sử dụng mật khẩu này cho một trong các tài khoản của mình bởi những người trong nhóm sẽ biết.

Học viên có 5 phút để thực hiện. Sau đó, hãy hỏi một vòng quanh phòng, yêu cầu học viên đưa ra ví dụ về các mật khẩu mà họ cho là mạnh nhất. Hỏi học viên xem liệu họ có thể nhớ các mật khẩu đã tạo nếu không nhìn chúng hay không.

Mặc dù có vài trang web sẽ yêu cầu mật khẩu của chúng ta phải đáp ứng một số (hoặc tất cả) các điều kiện này, nhưng cũng có các trang không. Chúng ta cũng có thể tạo mật khẩu bằng một chuỗi các từ ngẫu nhiên thông dụng.

Tương tác trong lớp

Hãy yêu cầu các cặp tạo mật khẩu mới là các chuỗi từ. Cho họ biết mật khẩu nên có ít nhất 4 từ, như thế mật khẩu sẽ vừa mạnh lại vừa dễ nhớ. Học viên có 5 phút để thực hiện. Sau đó theo vòng tròn, yêu cầu học viên chia sẻ các ví dụ mật khẩu của họ. Nhắc lại cho học viên nhớ rằng tờ giấy đó sẽ không được thu lại khi kết thúc hoạt động, đồng thời họ không nên dùng mật khẩu đã cung cấp trong hoạt động cho bất kỳ tài khoản nào của mình.

Nói với học viên

Một số trang web sử dụng hệ thống xác thực nhiều yếu tố (hoặc hai yếu tố) để xác minh danh tính của chúng ta. Những trang web này thường sử dụng tin nhắn văn bản, ứng dụng hoặc email để gửi mã dùng một lần mà chúng ta phải nhập cùng với mật khẩu.

Phương pháp này có thể giữ cho tài khoản của chúng ta an toàn hơn nhiều bằng cách thêm một lớp bảo mật bổ sung cực kỳ khó phá vỡ. Ví dụ: để đăng nhập vào tài khoản của chúng ta, một người phải có mật khẩu và quyền truy cập vào ứng dụng, thiết bị hoặc địa chỉ email liên kết với tài khoản đó.

Giữ mật khẩu an toàn

Phần 1

Nói với học viên

Ngay cả khi chúng ta tạo một mật khẩu thực sự khó đoán đối với máy tính hoặc người muốn bẻ khóa, thì vẫn có những cách khác làm suy yếu mật khẩu.

Hỏi học viên

Vậy khi nào thì một mật khẩu còn bị xem là yếu?

1. Đó là sử dụng lại một mật khẩu cho nhiều tài khoản, sử dụng một mật khẩu chứa thông tin cá nhân, sử dụng cùng một mật khẩu trong nhiều năm, quên mật khẩu.

Chúng ta cho rằng mình nên thay đổi mật khẩu bao lâu một lần?

Nói với học viên

Ngay cả những mật khẩu mạnh cũng có thể bị xâm phạm hoặc đánh cắp. Tuy nhiên, có một số cách để chúng ta bảo vệ chính mình. Nếu một trang web mà chúng ta có tài khoản bị xâm phạm dữ liệu, hãy đảm bảo đổi mật khẩu trên trang web đó cũng như bất kỳ trang nào chúng ta sử dụng mật khẩu tương tự.

Có thể chúng ta sẽ gặp khó khăn khi phải nhớ nhiều mật khẩu dài và phức tạp.

Hỏi học viên

Chúng ta có nghĩ mình nên viết mật khẩu ra giấy hay lưu trong một file tài liệu trên máy tính không? Tại sao có, tại sao không?

Tương tác trong lớp

Đề cập đến khả năng ai đó tìm thấy tờ giấy này hoặc nhìn thấy file trên máy tính. Giải thích rằng có một cách đó là sử dụng trình quản lý mật khẩu, một ứng dụng giúp người dùng lưu và sắp xếp mật khẩu của họ.

Phần 2

Nói với học viên

Hàng ngày, chúng ta sử dụng nhiều tài khoản trên những trang web khác nhau. Vì vậy, mỗi lần đăng nhập và đăng xuất khỏi từng trang web có thể khiến chúng ta thấy

thật phiền phức.

Hỏi học viên

Chúng ta đã bao giờ sử dụng tính năng “lưu mật khẩu” trong trình duyệt để lưu mật khẩu cho một trang web chưa? Tại sao có, tại sao không?

Chúng ta có hiểu cách trang web ghi nhớ danh tính của mình không?

1. Hãy đề nghị học viên giải thích. Sau đó, giảng giải rằng trang web có thể ghi nhớ việc chúng ta đã đăng nhập bằng cách lưu trữ cookie. Cookie là các tệp nhỏ được lưu trữ trên máy tính để sau này khi truy cập lần nữa, trang web nhận ra chúng ta và máy tính mà không cần đăng nhập lại. Tuy nhiên, cookie cũng có thể được sử dụng để theo dõi chúng ta khi chúng ta chuyển từ trang web này sang trang web khác. Đó là một cách để quảng cáo có thể nhắm mục tiêu đến chúng ta.

Có nên lưu mật khẩu trên máy tính của chúng ta không?

Hỏi học viên

Máy tính của chúng ta có mật khẩu đăng nhập không?

Vậy lỡ chúng ta cho người khác dùng chung máy tính đó thì thế nào?

1. Khi đó, cho dù mật khẩu của chúng ta hiển thị dưới dạng các dấu chấm đen hoặc dấu hoa thị, thì những người dùng chung máy tính với chúng ta vẫn có khả năng đoán ra nó. Chúng ta không nhìn thấy mật khẩu trên màn hình chẳng có nghĩa là mật khẩu không được lưu trữ ở đâu đó.

Hỏi học viên

Chúng ta có thể chia sẻ mật khẩu trong những trường hợp nào? Khi nào? Tại sao?

1. Đó là khi cha mẹ muốn biết mật khẩu của học viên hoặc học viên có một tài khoản gia đình/dùng chung trên một dịch vụ như Netflix chẳng hạn.

Chúng ta có chia sẻ mật khẩu với bất kỳ ai không? Nếu có, người đó là ai/tại sao?

Nếu chúng ta là bạn thân của ai đó, họ có đặt ra điều kiện “nếu cậu quan tâm đến mình” để gây sức ép khiến chúng ta chia sẻ mật khẩu với họ không? Tại sao có, tại sao không?

Nói với học viên

Chúng ta có thể chọn cách chia sẻ mật khẩu của mình với người nào đó mà chúng ta quan tâm. Tuy nhiên, quan tâm đến một người không nhất thiết là phải trao cho họ toàn quyền truy cập vào tài khoản trên mạng của chúng ta.

Hãy suy nghĩ kỹ về mối quan hệ của chúng ta với người đó trước khi chia sẻ, kể cả việc mối quan hệ này có thể sẽ thay đổi theo thời gian. Ví dụ: chọn chia sẻ với cha mẹ/người chăm sóc là rất khác so với việc chia sẻ với bạn thân.

Hỏi học viên

Điều gì có thể xảy ra nếu chúng ta chia sẻ mật khẩu?

1. Ai đó có thể hack tài khoản ngân hàng của chúng ta, mạo danh chúng ta trên mạng hoặc nắm được một số bí mật của chúng ta.

Nếu đã chia sẻ mật khẩu của một tài khoản, chúng ta có sử dụng tài khoản đó theo cách khác không?

Hỏi học viên

Nếu ai đó biết chúng ta đang làm gì, thì thế nào cũng có những nội dung chúng ta sẽ không xem trên Netflix hoặc không viết ra email, đúng không?

Tương tác trong lớp

Hãy để học viên suy ngẫm về hành vi của chính họ khi sử dụng tài khoản chung. Họ nên lưu ý rằng những người khác dùng chung tài khoản đó sẽ biết được họ làm gì trên mạng.

Hỏi học viên

Nếu tài khoản của chúng ta đại diện cho chúng ta trên mạng, chẳng hạn như trang cá nhân trên mạng xã hội, thì chúng ta có nên cho người khác sử dụng tài khoản đó không?

Tương tác trong lớp

Hãy bàn đến khả năng ai đó có thể mạo danh chúng ta rồi nhắn tin cho bạn bè của chúng ta.

Hỏi học viên

Chúng ta có cho phép bất kỳ thiết bị nào mà chúng ta sử dụng lưu trữ mật khẩu của mình không? Tại sao có, tại sao không? Như vậy có nghĩa là lưu mật khẩu trên điện thoại hoặc máy tính cá nhân thì an toàn, phải không? Điều gì sẽ xảy ra nếu chúng ta cho bạn bè mượn điện thoại hoặc máy tính?

Chúng ta có dùng chung bất kỳ thiết bị nào với người khác, chẳng hạn như với gia đình hoặc bạn bè không? Chúng ta có chia sẻ tài khoản trên thiết bị đó không hay mỗi người có một tài khoản riêng?

Chúng ta đã từng sử dụng thiết bị “công cộng”, chẳng hạn như tại thư viện, trường học hay nơi nào khác chưa? Trên thiết bị đó, chúng ta có làm những việc tương tự như trên các thiết bị khác không?

Phần 3

Tương tác trong lớp

Chia học viên thành các cặp.

Nói với học viên

Theo cặp, chúng ta hãy thảo luận xem mình đã từng đăng nhập vào máy tính tại trường học, thư viện hay ở một nơi công cộng nào khác chưa và có nhìn thấy ai đó vẫn chưa đăng xuất khỏi tài khoản Mạng xã hội hoặc tài khoản email của họ không. Yêu cầu học viên suy nghĩ xem họ có ngó nghiêng tài khoản đó hay làm gì khác không.

Tương tác trong lớp

Hãy dành cho học viên 5 phút để thảo luận, sau đó đề nghị họ chia sẻ ý kiến. Yêu cầu nhóm thảo luận về việc sử dụng trái phép này.

Truy cập trái phép vào tài khoản

Phần 1

Tương tác trong lớp

Lưu ý: Một phần nội dung trong hoạt động này đã được đề cập ở “Hoạt động số 1: Thông tin cơ bản về mật khẩu”. Tùy bạn đánh giá xem mình có cần lặp lại nội dung này không hay sẽ bỏ qua.

Nói với học viên

Người khác có thể truy cập vào tài khoản của chúng ta ngay cả khi chưa biết hoặc không đoán đại được mật khẩu. Nếu một người nắm đủ thông tin cá nhân về chúng ta thì có thể dựa vào đó để đoán ra mật khẩu. Họ cũng có thể thuyết phục một ai đó ở công ty liên quan cung cấp thông tin của chúng ta. Do không sử dụng công nghệ để xâm nhập tài khoản nên loại hình tấn công này gọi là lừa đảo mạo danh (social hacking) hoặc lừa đảo qua mạng (social engineering).

Hỏi học viên

Ai đã từng quên mật khẩu dùng để truy cập vào một trang web thì giơ tay lên nào.

Điều gì sẽ xảy ra khi chúng ta nhấp vào dòng chữ “Quên mật khẩu?”

1. Trang web thường yêu cầu chúng ta trả lời các câu hỏi bảo mật hoặc cố gắng liên hệ với chúng ta qua điện thoại hoặc email.

Một số câu hỏi bảo mật mà trang web thường hỏi là gì?

1. Giải thích tại sao bạn bè hoặc người quen có thể trả lời hoặc đoán ra một vài câu hỏi trong số này. Những câu hỏi như: tên thú cưng, nơi sinh, tên thời con gái của mẹ, tên giáo viên yêu thích, tên người bạn tốt nhất, tên đội tuyển thể thao yêu thích.

Những ai khác có thể biết loại thông tin này về chúng ta?

Trang web liên hệ với chúng ta bằng cách nào khi chúng ta quên mật khẩu?

Những ai khác có thể truy cập được vào các đầu mối liên hệ này?

Hỏi học viên

Bằng cách nào mà một người lạ biết được thông tin cá nhân liên quan đến đáp án

cho câu hỏi bảo mật của chúng ta?

1. Qua bài viết trên mạng xã hội, lên mạng tìm kiếm thông tin công khai, đoán đi đoán lại nhiều lần, liên hệ với bạn bè chúng ta, v.v.

Hãy nêu một số ví dụ về bài viết trên mạng xã hội chứa thông tin cá nhân?

1. Ví dụ: một bài viết trên Instagram về em mèo mình nuôi và có chú thích tên nó, một bức ảnh gắn thẻ vị trí hoặc bài viết về ngày sinh nhật ở chế độ công khai.

Chúng ta có thể tận dụng Google để tìm hiểu thêm về một người và hack mật khẩu của họ như thế nào?

1. Nếu một công cụ tìm kiếm hiển thị cho chúng ta bức ảnh hồi lớp 9 của ai đó trên tờ báo mạng của trường, thì chúng ta có thể tìm ra tên giáo viên dạy họ năm đó.

Phần 2

Nói với học viên

Đăng thông tin chứa đáp án cho các câu hỏi bảo mật của chúng ta là một hành động không an toàn chút nào. Hãy đảm bảo chọn các câu hỏi bảo mật mà chỉ duy nhất bản thân mình mới trả lời được. Chúng ta cũng có thể bịa ra câu trả lời cho các câu hỏi bảo mật, miễn là có lưu lại trong trình quản lý mật khẩu hoặc là chúng dễ nhớ.

Các trang web có thể liên hệ với người dùng bằng số điện thoại hoặc email liên kết với tài khoản của người dùng đó. Nếu người dùng quên mật khẩu, các trang web thường cung cấp một mật khẩu tạm thời hoặc siêu liên kết để người dùng đặt lại mật khẩu.

Hỏi học viên

Đây có phải là cách an toàn để đảm bảo rằng người yêu cầu mật khẩu mới cũng chính là người dùng không?

Điều gì sẽ xảy ra nếu chúng ta chia sẻ địa chỉ email được liên kết với tài khoản đó?

1. Sử dụng liên kết đặt lại mật khẩu thường là phương pháp an toàn, nhưng sẽ khá rủi ro nếu chúng ta dùng chung tài khoản hoặc mật khẩu với ai khác.

Nói với học viên

Kẻ xấu có thể lừa đảo mạo danh bằng cách liên hệ trực tiếp với chúng ta và cố gắng

lừa chúng ta cung cấp thông tin. Đôi khi, kẻ xấu sẽ mạo danh người khác (chẳng hạn như bạn bè, người nhà hoặc nhân viên ngân hàng) gửi email và yêu cầu chúng ta chia sẻ thông tin quan trọng với chúng (chẳng hạn như ngày sinh) để từ đó xác minh danh tính của ta. Sẽ lại càng tinh vi hơn nữa nếu ai đó hack tài khoản mạng xã hội của bạn bè rồi nhắn tin cho chúng ta (và cũng có thể là cho nhiều người khác) để hỏi ngày sinh nhật hoặc nơi chúng ta lớn lên. Nếu nhận được bất kỳ tin nhắn nào của bạn bè mà có vẻ khác thường, trước tiên chúng ta cần liên lạc với người bạn này (bằng các phương tiện khác chứ không phải qua nền tảng mạng xã hội) để xác định xem họ có đang thực sự gửi nội dung đó không.

Các hình thức tấn công bằng cách sử dụng email hoặc trang web trông như thật được gọi là lừa đảo phishing và có thể dùng để đánh cắp danh tính. Ví dụ: một kẻ đánh cắp danh tính có thể mở và dùng thẻ tín dụng dưới tên chúng ta. Như vậy khi lớn lên, chúng ta sẽ khó mở được thẻ tín dụng.

Lừa đảo phishing được rồi thì kẻ cắp sẽ mạo danh chúng ta và truy cập nhiều thông tin khác. Từ đó chúng sẽ xem trộm email của ta, giả vờ là ta để nhắn tin cho bạn bè ta hoặc lấy cắp cả tiền của chúng ta nữa. Ngoài ra trong quá trình này, kẻ đánh cắp danh tính cũng có thể ngăn chặn chúng ta truy cập vào tài khoản của chính mình bằng cách tạo mật khẩu mới mà chúng ta không biết.

Bài tập

Phiếu bài tập

Bài tập

Yêu cầu học viên điền câu trả lời của mình dưới dạng văn bản hoặc hình ảnh vào phiếu bài tập Tìm hiểu về mật khẩu.

1. Bạn sẽ áp dụng 3 kết luận nào của bài học này khi phải tạo mật khẩu trong tương lai?

2. Ví dụ một trường hợp mà bạn cảm thấy nên chia sẻ mật khẩu của mình với ai đó?

3. Có ba chiến lược nào để bạn chia sẻ mật khẩu của mình với người khác một cách an toàn?

4. Hãy nêu ba ví dụ về hậu quả nếu như mật khẩu rơi vào tay kẻ xấu?