BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU THUYẾT MINH CHUYÊN ĐỀ "KIẾN THỨC, KỸ NĂNG BẢO ĐẢM AN TOÀN THÔNG TIN KHI SỬ DỤNG THƯ ĐIỆN TỬ VÀ GIAO DỊCH TRỰC TUYẾN"

Hà Nội, năm 2023

1. HƯỚNG DẪN GIAO DỊCH, THANH TOÁN TRỰC TUYẾN AN TOÀN

1.1 Vai trò của giao dịch, thanh toán trực tuyến

Thay vì dùng tiền mặt như trước đây, các cửa hàng, siêu thị, nhà hàng, quán ăn quy mô lớn đều dần chuyển sang thanh toán điện tử. Điều này mang đến nhiều sự thuận tiện cho cả người mua và người bán.

1.2. Cảnh báo các thủ đoạn gian lận thường gặp

a) Lừa khách hàng tự chuyển tiền

Đối tượng gian lận thường chủ động liên hệ với khách hàng qua điện thoại, mạng xã hội hoặc email với các nội dung như:

- Giả mạo cơ quan điều tra thông báo liên quan đến một vụ án bất kỳ và yêu cầu khách hàng chuyển tiền để phục vụ điều tra.

- Giả mạo thông báo trúng thưởng từ ngân hàng hoặc các công ty lớn.

- Giả mạo người thân, bạn bè nhờ chuyển tiền hộ.

b) Đánh cặp thông tin bảo mật từ khách hàng

Đây là hành vi của cá nhân, tổ chức thu thập các thông tin cá nhân của khách hàng để kiếm các lợi ích tài chính cho bản thân thông qua các phương thức:

- Yêu cầu cung cấp thông tin bảo mật của Ngân hàng điện tử hoặc thẻ và chuyển mã OTP cho đối tượng lừa đảo.

- Hướng dẫn truy cập website của dịch vụ chuyển tiền, nhập thông tin đăng nhập tài khoản ngân hàng, hoặc thông tin thẻ để nhận tiền. Thực chất đây là các website giả mạo.

- Lừa khách hàng cài đặt các phần mềm/ứng dụng gián điệp để đánh cắp thông tin từ tin nhắn hoặc khi khách hàng đăng nhập website của ngân hàng.

- Lưu trữ trái phép các thông tin thẻ và dịch vụ ngân hàng đã nhập của khách hàng trên website có rủi ro cao.

c) Một số hình thức lừa đảo:

Giả mạo email từ ngân hàng, thông báo tài khản bị trừ tiền (hoặc được cộng tiền trúng thưởng chẳng hạn) và đưa đường link đăng nhập, nhưng thực chất là đường link giả có giao diện giống với trang web của ngân hàng thật. Khi bạn sơ ý nhập thông tin tài khoản, mật khẩu vào, chúng sẽ bị đánh cắp.

1.3. Hướng dẫn thanh toán trực tuyến an toàn

Để thanh toán trực tuyến an toàn, cụ thể là thanh toán trực tuyến qua dịch vụ e-banking, Internet banking của các tài khoản ngân hàng, thẻ ATM, thẻ VISA,… cũng như tránh bị đánh cắp thông tin thanh toán, mọi người cần phải tuân thủ một số nguyên tắc cơ bản.

a) Sử dụng cổng giao dịch "chính hãng"

Khi sử dụng dịch vụ ngân hàng trực tuyến, tuyệt đối không thực hiện gián tiếp thông qua các đường link nhận được từ email/tin nhắn hoặc trên trang Web nào đó tạo ra mà phải truy cập trực tiếp vào trang chủ ngân hàng để thực hiện giao dịch.

b) Giữ bí mật thông tin cá nhân

Tuyệt đối giữ bảo mật thông tin tài khoản ngân hàng như: số thẻ, số tài khoản và tên truy cập dịch vụ ngân hàng điện tử qua Internet, Mobile,… Tuyệt đối giữ bảo mật các thông tin cá nhân như: họ và tên, địa chỉ, ngày sinh, số CMND.

Các thông tin này thường được khai thác qua nhiều hình thức như:

- Được trúng thưởng,

- Được tặng quà,

- Dò hỏi người thân,

- Hù dọa (Hù dọa thiếu cước viễn thông, nợ ngân hàng, hù bị ai rút tiền,…).

Cách đối phó là đừng cung cấp thông tin thật hoặc kiểm tra lại thông tin với ngân hàng bằng cách liên lạc qua số điện thoại hỗ trợ chính thức mà mình biết.

c) Đặt mật khẩu an toàn

Hãy đặt mật khẩu thật an toàn cho tài khoản Internet Banking. Nếu được, hãy đổi mật khẩu này định kỳ.

d) Sử dụng dịch vụ tin nhắn chủ động

Nên đăng ký sử dụng dịch vụ nhắn tin, truy vấn số dư chủ động (SMS Banking) để có thể chủ động theo dõi được những biến động số dư trên tài khoản tiền gửi hoặc thẻ thanh toán nhằm phát hiện và xử lý kịp thời khi có các thanh toán bất thường.

đ) Đăng ký sử dụng OTP

OTP là mật khẩu sử dụng một lần, nó tạo ra rào an ninh vô cùng mạnh bằng cách nhắn tin đến số điện thoại của bạn một mậu khẩu xác thực trước khi phê duyệt và thực hiện giao dịch.

Vì vậy, khi kẻ xấu có hầu hết thông tin ngân hàng của bạn và tiến hành thanh toán bằng tài khoản này, một mật khẩu OTP sẽ được gửi qua điện thoại bạn đang cầm để xác thực.

Giao dịch sẽ thành công chỉ khi nào kẻ xấu cũng có được OTP này. Do đó, kẻ xấu sẽ không thể thực hiện giao dịch với tài khoản của bạn trừ khi bạn mất điện thoại và để lọt vào tay kẻ xấu đó hoặc cao hơn là bị hack/virus đọc được tin nhắn OTP.

2. BẢO ĐẢM AN TOÀN THÔNG TIN KHI SỬ DỤNG THƯ ĐIỆN TỬ

2.1. Đào tạo mọi người về các biện pháp bảo mật email tốt nhất

Đào tạo nhận thức bảo mật được lên lịch thường xuyên và thông báo cho mọi người về các phương pháp bảo mật tốt nhất, giúp người dùng cập nhật không chỉ các chính sách bảo mật của cơ quan cũng như vai trò của họ trong giữ an toàn cho tổ chức và những mối đe dọa mà họ có thể gặp phải.

Tổ chức các khóa đào tạo nâng cao nhận thức về bảo mật và giải thích chính sách bảo mật email của cơ quan, các mối đe dọa bảo mật email phổ biến và khuyến nghị các phương pháp hay nhất về bảo mật email.

2.2. Tạo mật khẩu mạnh

Một trong những biện pháp bảo mật email quan trọng nhất là sử dụng mật khẩu mạnh. Tuy nhiên, lời khuyên về bảo mật mật khẩu đã thay đổi trong những năm gần đây. Suy nghĩ trước đây cho rằng phức tạp đồng nghĩa với mạnh mẽ. Tuy nhiên, việc buộc mọi người tạo mật khẩu phức tạp thường kết thúc bằng việc người dùng viết mật khẩu của họ vào một tờ giấy dán hoặc lưu chúng vào một tệp không an toàn trên máy tính để bàn của họ.

Khuyến nghị hiện tại của TỔ CHỨC TIÊU CHUẨN CỦA MỸ là độ dài mật khẩu chứ không phải độ phức tạp mới là chìa khóa cho độ an toàn của mật khẩu. Cụm mật khẩu, việc xâu chuỗi một vài từ lại với nhau là một phương pháp tạo mật khẩu dài hơn, dễ nhớ nhưng khó đoán, giúp chống lại những kẻ tấn công sử dụng từ điển để nhắm mục tiêu mật khẩu yếu.

2.3. Không sử dụng lại mật khẩu trên nhiều tài khoản

Sử dụng lại mật khẩu là mối đe dọa bảo mật email lớn. Nếu kẻ tấn công xâm phạm một tài khoản sử dụng thông tin đăng nhập giống như các tài khoản khác thì kẻ tấn công có thể dễ dàng truy cập vào các tài khoản khác đó. Việc sử dụng lại mật khẩu đặc biệt nguy hiểm khi cá nhân sử dụng cùng một mật khẩu cho tài khoản cơ quan và cá nhân.

Khuyến khích mọi người tuân theo các phương pháp hay nhất về bảo đảm an toàn mật khẩu, chẳng hạn như sử dụng mật khẩu mạnh, duy nhất cho mỗi tài khoản. Đây là điểm khó khăn đối với nhiều người dùng, đặc biệt là những người có hàng chục hoặc hàng trăm tài khoản. Việc sử dụng đăng nhập một lần hoặc trình quản lý mật khẩu có thể giúp giảm bớt thách thức.

2.4. Cân nhắc việc thay đổi mật khẩu thường xuyên - hoặc không

Hướng dẫn về tần suất thay đổi mật khẩu đã được tranh luận trong những năm gần đây. Thay đổi mật khẩu 90 ngày một lần đã là điều bình thường. Giả định rằng việc thay đổi mật khẩu thường xuyên giúp giữ an toàn cho hệ thống, nhưng chúng thường khiến người dùng thất vọng và sử dụng mật khẩu kém an toàn hơn. Thông thường, Password1 sẽ chuyển thành Password2 sau 90 ngày.

TỔ CHỨC TIÊU CHUẨN CỦA MỸ không khuyến nghị buộc thay đổi mật khẩu định kỳ. Tuy nhiên, hãy luôn buộc thay đổi mật khẩu sau khi nghi ngờ có sự xâm phạm hoặc vi phạm dữ liệu. Ngoài ra, một số quy định tuân thủ, chẳng hạn như PCI DSS, yêu cầu thay đổi mật khẩu thường xuyên.

Các cơ quan phải cân nhắc lợi ích của việc thay đổi mật khẩu thường xuyên với người dùng; xu hướng sử dụng mật khẩu yếu hơn, dễ nhớ hơn và do đó kẻ tấn công dễ khai thác hơn.

2.5. Sử dụng xác thực đa yếu tố

MFA: Sử dụng nhiều phương pháp để xác thực danh tính của người dùng. Ví dụ: tên người dùng và mật khẩu kết hợp với mật khẩu dùng một lần hoặc dấu vân tay sinh trắc học. Việc thêm yếu tố thứ hai hoặc thứ ba hoặc nhiều hơn vào quy trình xác thực sẽ thêm một lớp bảo vệ bổ sung và bảo vệ chống lại các mối đe dọa email phổ biến, chẳng hạn như các cuộc tấn công và bẻ khóa mật khẩu. Microsoft đã dự đoán khóa tài khoản bằng MFA có thể chặn 99,9% các cuộc tấn công xâm phạm tài khoản.

Các cơ quan nên bắt buộc sử dụng MFA. Cá nhân cũng nên bảo vệ tài khoản cá nhân của mình bằng cách sử dụng MFA bất cứ khi nào có sẵn.

2.6. Hãy coi trọng việc lừa đảo

Mặc dù các sản phẩm bảo mật email ngăn nhiều email spam tiếp cận hộp thư đến của người dùng nhưng một lượng lớn thư rác vẫn lọt qua được và có thể chứa các âm mưu lừa đảo ngày càng trở nên tinh vi. Chúng có thể bao gồm các email lừa đảo cơ bản, cùng với các cuộc tấn công lừa đảo trực tuyến. Người dùng nên cảnh giác với các hành vi lừa đảo và thận trọng khi mở bất kỳ email độc hại tiềm ẩn nào. Không mở, trả lời, nhấp vào liên kết trong hoặc mở tệp đính kèm từ các email có vẻ đáng ngờ.

Ngày càng có nhiều tổ chức đưa chương trình đào tạo nâng cao nhận thức về lừa đảo vào các chương trình đào tạo nâng cao nhận thức về bảo mật của họ để giúp nhân viên xác định các thư có vấn đề và hướng dẫn họ cách tránh nhấp vào sai liên kết hoặc mở nhầm tệp đính kèm.

2.7. Hãy cảnh giác với các tệp đính kèm email

Nhiều cuộc tấn công qua email dựa vào khả năng gửi và nhận các tệp đính kèm có chứa mã độc. Cổng bảo mật email và phần mềm chống phần mềm độc hại có thể phát hiện các nguồn độc hại và chặn hầu hết các nguồn độc hại tệp đính kèm. Tuy nhiên, những tệp đính kèm này cũng có thể đến từ các nguồn đáng tin cậy đã bị kẻ tấn công khai thác.

Dù nguồn nào, nhân viên cũng nên cẩn thận với các tệp đính kèm ngay cả khi tổ chức sử dụng phần mềm quét email và chặn phần mềm độc hại. Hãy hết sức thận trọng trước khi mở tệp đính kèm có phần mở rộng được liên kết với chương trình thực thi, chẳng hạn như EXE (tệp thực thi), JAR (tệp ứng dụng Java) hoặc MSI (Trình cài đặt Windows). Các tệp như tài liệu Word, Exel và PDF cũng có thể mang mã độc, vì vậy hãy cẩn thận khi xử lý mọi loại tệp đính kèm. Quét tệp bằng chương trình chống phần mềm độc hại hoặc tránh mở chúng hoàn toàn.

2.8. Đừng nhấp vào liên kết email

Các liên kết trong email thường có thể kết nối với một tên miền trang web khác với miền mà chúng đại diện. Một số liên kết có thể hiển thị một tên miền trang web dễ nhận biết nhưng trên thực tế, hướng người dùng đến một tên miền trang web độc hại khác. Những kẻ tấn công cũng sử dụng các bộ ký tự quốc tế hoặc lỗi chính tả để tạo ra các miền độc hại.

Luôn xem lại nội dung liên kết bằng cách di con trỏ chuột lên liên kết để xem liên kết thực tế có khác với liên kết hiển thị hay không. Tuy nhiên, hãy lưu ý rằng ngay cả điều này cũng có thể bị giả mạo, mặc dù hầu hết các chương trình email hiện đại đều có thể ghi nhận được các liên kết như vậy. Khi nghi ngờ, hãy nhập tên miền trang web trực tiếp vào trình duyệt để tránh nhấp vào liên kết trong email.

2.9. Không sử dụng email công việc cho mục đích cá nhân và ngược lại

Mặc dù việc nhân viên sử dụng tài khoản email cơ quan cho các vấn đề cá nhân có thể hấp dẫn và thuận tiện, nhưng cách tốt nhất để bảo mật email cơ quan là cấm hành vi này. Tương tự, không gửi email liên quan đến công việc từ tài khoản cá nhân. Việc kết hợp các vấn đề kinh doanh và cá nhân có thể dẫn đến các mối đe dọa như lừa đảo trực tuyến.

2.10. Chỉ sử dụng email công việc trên các thiết bị được phê duyệt

Mọi người có thể truy cập email từ bất cứ đâu và trên bất kỳ thiết bị kết nối internet nào. Mặc dù thuận tiện cho nhân viên nhưng điều này có thể trở thành thảm họa an an toàn thông tin cho một tổ chức. Nếu email cơ quan được mở trên các thiết bị không có biện pháp kiểm soát bảo mật thích hợp, kẻ tấn công có thể lấy cắp thông tin của người dùng, thông tin xác thực, email và dữ liệu.

2.11. Mã hóa email, thông tin liên lạc và tệp đính kèm

Người ta nói rằng email giống như một tấm bưu thiếp: Mọi người và hệ thống mà nó tiếp xúc đều có thể xem những gì được viết. Đây là lý do tại sao email mã hóa lại quan trọng đến vậy. Mã hóa, quá trình chuyển đổi văn bản gốc thành văn bản mã hóa, đảm bảo rằng bất kỳ ai chặn email đều không thể đọc được nội dung của nó. Điều này giúp ngăn chặn nhiều vấn đề bảo mật email . Hầu hết các ứng dụng email lớn đều có khả năng mã hóa.

Tuy nhiên, việc mã hóa tin nhắn thôi là chưa đủ. Đồng thời mã hóa thông tin liên lạc giữa tổ chức và nhà cung cấp email. Mã hóa các tệp đính kèm, ngay cả khi email đính kèm chúng được mã hóa.

2.12. Tránh Wi-Fi công cộng

Nhân viên có thể coi Wi-Fi công cộng là một điều may mắn, nhưng họ nên được nhắc nhở rằng những kết nối này đã sẵn sàng cho các cuộc tấn công. Nếu nhân viên đăng nhập vào email công ty trên Wi-Fi công cộng thì bất kỳ ai trên mạng đó cũng có thể truy cập email của họ. Những kẻ độc hại có thể sử dụng các

phần mềm rà quét mã nguồn mở để theo dõi và giành quyền truy cập vào thông tin cá nhân qua email. Ngay cả khi người dùng không chủ động kiểm tra email trên Wi-Fi công cộng, hầu hết mọi hệ thống đều được đặt để tự động cập nhật hộp thư đến khi thiết bị kết nối với mạng. Nếu người dùng sử dụng Wi-Fi thì email của họ cũng vậy, khiến thông tin đăng nhập tài khoản gặp rủi ro.

2.13. Sử dụng giao thức bảo mật email

03 tiêu chuẩn bảo mật email để lọc thư rác:

- Thư được xác định bằng khóa miền: Tiêu chuẩn DKIM sử dụng mật mã bất đối xứng để ngăn chặn việc giả mạo email. Chữ ký điện tử được thêm vào email sẽ xác minh thư không bị thay đổi sau khi được gửi. Nếu chữ ký không khớp với khóa chung của miền email thì nó sẽ bị chặn. Nếu khớp thì nó sẽ được gửi.

Khung chính sách người gửi: SPF xác minh email đến từ nguồn của nó và được phép gửi email từ miền đó. Nếu được xác minh, email sẽ được gửi. Nếu không, email sẽ bị chặn.

Xác thực, báo cáo và tuân thủ thư dựa trên tên miền trang web: Giao thức DMARC mở rộng DKIM và SPF. Bằng cách sử dụng DMARC, chủ sở hữu miền có thể công bố các yêu cầu về DKIM và SPF, cũng như chỉ định điều gì sẽ xảy ra khi email không đáp ứng được các yêu cầu đó, chẳng hạn như báo cáo lại cho miền gửi.

2.14. Sử dụng các công cụ bảo mật email

Ngoài việc triển khai các phương pháp phù hợp, chiến lược bảo mật email nên bao gồm nhiều công cụ giúp duy trì bảo mật email. Cần xem xét phần mềm chống phần mềm độc hại, chống thư rác, chống vi-rút, lọc email, cổng bảo mật email, hệ thống giám sát email, tường lửa và bảo vệ thiết bị đầu cuối.

2.15. Đăng xuất

Yêu cầu nhân viên đăng xuất khỏi email khi không sử dụng và khi đã hoàn thành công việc trong ngày. Để email mở trên các thiết bị mà người khác có thể truy cập được có thể dẫn đến các vấn đề về mất an toàn thông tin.

Hướng dẫn xác thực hai yếu tố thư điện tử

Kích hoạt 2FA trên tài khoản email: Đăng nhập vào tài khoản email của

bạn và tìm đến cài đặt bảo mật hoặc quản lý tài khoản. Tìm tùy chọn 2FA hoặc Xác thực hai yếu tố và bật nó.

Bước 1: Truy cập vào trang https://myaccount.google.com/security và đăng nhập tài khoản Gmail.

Bước 2: Sau khi đăng nhập ta sẽ thấy phần xác minh 2 bước như hình dưới đang ở trạng thái tắt, bạn nhấn vào để bật.

Bước 3: Sau khi nhấn vào, cửa sổ sẽ hiện ra và ta chọn BẮT ĐẦU.

Bước 4: Để bật tính năng này bạn cần phải xác minh một lần nữa bằng cách nhập mật khẩu của bạn và nhấn Tiếp theo.

Bước 5: Sau khi đã xác minh. Bạn cần phải xác minh thêm một lần nữa bằng số điện thoại để bật tính năng này. Bạn cần chọn số điện thoại, cách nhận mã rồi sau đó nhấn GỬI

Bước 6: Sau khi nhận được mã được gửi qua số điện thoại, bạn điền vào ô Nhập mã rồi nhấn TIẾP THEO

Bước 7: Hoàn tất bật xác minh 2 bước bằng cách nhấn vào nút BẬT..

3. HƯỚNG DẪN SỬ DỤNG INTERNET, MẠNG XÃ HỘI AN TOÀN

3.1. Tại sao cần đảm bảo an toàn sử dụng Internet

Tình hình sử dụng các công nghệ số (kỹ thuật số) tại Việt Nam trong năm 2023, tập trung chính vào Internet và những thay đổi, xu hướng liên quan đến việc sử dụng các công nghệ số.

Đầu năm 2023, Việt Nam có 77,93 triệu người dùng Internet, chiếm 79,1% tổng dân số. Ngoài ra, số lượng người dùng mạng xã hội cũng đạt con số 70 triệu, tương đương với 71% tổng dân số. Tổng số kết nối di động đang hoạt động là 161,6 triệu, tương đương với 164,0% tổng dân số.

Dữ liệu này cho thấy Việt Nam có tổng số người dùng Internet và mạng xã hội đáng kể, cùng với số lượng kết nối di động vượt quá tổng dân số. Điều này cũng đồng nghĩa với việc tăng khả năng rủi ro về an ninh mạng.

Với số lượng người dùng lớn, các hệ thống như website, ứng dụng hoặc email doanh nghiệp trở thành mục tiêu hấp dẫn cho các tấn công và vi phạm bảo mật. Do đó, việc đảm bảo an ninh mạng là một thách thức mà các doanh nghiệp và tổ chức cần quan tâm. Để giảm thiểu rủi ro, các doanh nghiệp cần áp dụng các giải pháp CNTT, an ninh mạng chất lượng.

3.2. Làm thế nào để đảm bảo an toàn trên môi trường trực tuyến

- Xác định xem thông tin cá nhân hoặc blog của bạn nên đặt chế độ công khai như thế nào

- Khi sử dụng các trang mạng xã hội hoặc viết blog, hãy cân nhắc về việc một số trang web sẽ tự động chuyển sang chế độ công khai cho tất cả người dùng Internet về những gì bạn đăng tải.

-Hãy tìm phần Cài đặt (Settings) hoặc Tùy chọn (Options) để quản lý ai có thể thấy thông tin cá nhân, hình ảnh, danh sách bạn bè, và mọi người có thể tìm ra trang cá nhân của bạn bằng cách nào, ai có thể bình luận hoặc làm sao để chặn những truy cập không mong muốn.

- Bảo mật những thông tin cá nhân nhạy cảm.

- Trước khi nhập một thông tin nhạy cảm, hãy xem trang web đó có là địa chỉ web an toàn tin cậy hay không bằng cách tìm dấu hiệu https và biểu tượng khóa đóng bên cạnh

- Không bao giờ cung cấp các thông tin nhạy cảm (như số tài khoản hay mật khẩu) hoặc gọi vào một số điện thoại theo yêu cầu trong email hoặc tin nhắn hay trên mạng xã hội.

- Suy nghĩ kỹ trước khi phản hồi cho việc xin tiền từ những đối tượng tự xưng là “thành viên gia đình”, đó thường là một trò lừa đảo.

- Nghiên cứu kỹ bất kỳ trang mạng xã hội nào trước khi bạn sử dụng chúng.

- Hãy đọc kỹ các điều khoản sử dụng. Trang web có quyền sở hữu thông tin của bạn không? Có thể bán thông tin của bạn không? Hoặc dùng những thông tin cá nhân của bạn để gửi thông tin quảng cáo không?

- Tìm hiểu khả năng quản lý những tương tác lạm dụng và nội dung không phù hợp của trang web, cũng cách thức báo cáo những vấn đề đó với trang web có được đảm bảo không

- Cẩn thận khi lựa chọn bạn bè trên mạng

- Hãy nghĩ kỹ trước khi bạn chấp nhận lời mời kết bạn của ai đó. Chỉ nên kết bạn với những người mà bạn hoặc bạn thân của bạn đã gặp trực tiếp hoặc với những người mà bạn có bạn chung với họ

- Định kỳ đánh giá lại những người có quyền truy cập vào thông tin của bạn. Danh sách bạn bè cũng có thể thay đổi theo thời gian.

- Kiểm tra lại những gì người khác viết về bạn. Hãy chắc chắn rằng họ không đăng những điều mà bạn không muốn chia sẻ như những bức ảnh cá nhân hoặc nơi ở của bạn. Bạn hoàn toàn có thể yêu cầu họ gỡ những thông tin đó xuống.

- Sử dụng trình duyệt web an toàn

- Đảm bảo bạn đang ở trang web đúng – ví dụ, khi đăng nhập vào trang web của ngân hàng, hãy đảm bảo đó không phải là trang giả mạo.

- Tìm các địa chỉ trang web có https (s viết tắt cho secure (an toàn)) và khóa đóng bên cạnh. (Khóa này cũng có thể xuất hiện phía dưới bên phải của cửa sổ). Không gõ thông tin nhạy cảm vào các cửa sổ web tự động xuất hiện.

- Tránh nhấp chuột vào các trạng thái "Agree", "OK" hoặc "I accept"

- Trên các banner quảng cáo, cửa sổ pop-up bất ngờ hiện ra với những cảnh báo hoặc đề nghị diệt vi rút và các phần mềm gián điệp, hoặc trên các trang web có vẻ bất hợp pháp và không chính thống.

- Thay vào đó, hãy nhấn Ctrl + F4 hoặc Ctrl + Alt trên bàn phím để đóng các cửa sổ này lại.

- Nếu các cửa sổ này không đóng, hãy nhấn ALT + F4 trên bàn phím để đóng trình duyệt web lại. Đóng tất cả các tabs và không lưu lại bất cứ một tabs nào cho lần khởi động trình duyệt tiếp theo.

3.3. Hướng dẫn bảo đảm an toàn tài khoản mạng xã hội Facebook và Zalo bằng kích hoạt xác thực hai yếu tố (2FA)

Xác thực hai yếu tố là một trong những cách mạnh nhất để bảo mật hồ sơ của bạn khỏi những lần đăng nhập không mong muốn. Khi ai đó cố gắng đột nhập vào tài khoản đã bật 2FA, họ không thể vào mà không có mã xác thực OTP. Vì mã được chuyển đến điện thoại của bạn nên chỉ bạn mới có thể đăng nhập.

a) Hướng dẫn kích hoạt xác thực hai yếu tố trên Facebook

Bước 1: Truy cập Facebook.com/settings

Bước 2: Chọn (Bảo mật và đăng nhập)

Bước 3: Chọn Xác thực 2 yếu tố) => Chọn Edit (Chỉnh sửa) => Nhập lại mật khẩu

Bước 4: Chọn (Dùng ứng dụng xác thực)

Bước 5: Tải ứng dụng xác thực của bên Thứ 3 (Google Authenticator, Microsoft Authenticator, trên điện thoại.

Bước 6: Hoàn tất cài đặt ứng dụng xác thực, mở và quét mã QR hoặc nhập mã hiển thị trên màn hình, bấm (Tiếp tục).

Bước 7: Nhập mã xác minh từ ứng dụng xác thực trên điện thoại vào hộp (Xác thực 2 yếu tố) => Bấm nút (Tiếp tục).

Đối với ứng dụng Facebook trên điện thoại:

Bước 1: Bấm hình ba thanh ngang phía trên góc phải của ứng dụng

Bước 2: Chọn (Cài đặt & quyền riêng tư)

Bước 3: Chọn (Cài đặt)

Bước 4: Chọn (Bảo mật và đăng nhập).

Bước 5: Chọn (Sử dụng xác thực hai yếu tố)

Bước 6: Chọn (Ứng dụng xác thực) trong phần (Phương thức xác thực) => Bấm t (Tiếp tục)

Bước 7: Tải ứng dụng xác thực của bên Thứ 3 (Google Authenticator, Microsoft Authenticator,…) trên điện thoại.

Bước 8: Nhập mã xác minh từ ứng dụng xác thực trên điện thoại vào hộp thoại (Xác thực 2 yếu tố) => Bấm nút (Tiếp tục).

Bước 9: Nhập lại mật khẩu Facebook để xác minh

Bước 10: Nhập lại mật khẩu Facebook để xác minh

Bước 11: Hiện thông báo (Xác thực 2 yếu tố đang bật) => Bấm nút (Xong).

b) Hướng dẫn bật xác thực hai yếu tố Zalo

Bước 1: Mở ứng Zalo trên thiết bị của mình và truy cập tab Cá nhân. Sau đó, nhấn vào biểu tượng bánh răng cài đặt nằm ở góc trên cùng bên phải.

Bước 2: Trong danh mục các Cài đặt, chạm vào Tài khoản và bảo mật.

Bước 3: Sau đó, bật công tắc chuyển đổi tại mục Xác thực 2 lớp để kích hoạt tính năng tăng cường bảo mật cho tài khoản Zalo của mình.

Bước 4: Nếu như muốn gỡ bỏ tính năng này, hãy gạt và tắt công tắc tại mục Xác thực 2 lớp.

Bước 5: Khi này, trên màn hình sẽ hiển thị khung cửa sổ thông báo “Tắt bảo mật 2 lớp”, hãy chạm vào nút Đồng ý

3.2. Kỹ năng thiết lập, quản lý, sử dụng mật khẩu an toàn

09 Quy tắc giúp thiết lập, quản lý mật khẩu an toàn

Sự an toàn của tài khoản ngân hàng, email, tài khoản nội bộ… của người dùng phụ thuộc vào cách người dùng bảo vệ mật khẩu của chính mình.

Quy tắc 1: Sử dụng trình quản lý mật khẩu để theo dõi mật khẩu

- Mật khẩu mạnh có đặc điểm dài hơn 8 ký tự, khó đoán, chứa nhiều loại ký tự, số và ký hiệu đặc biệt. Những mật khẩu tốt có thể khó nhớ, đặc biệt nếu người dùng sử dụng thông tin đăng nhập riêng biệt cho các trang web khác nhau (phương pháp được khuyến nghị). Đây là lý do mà trình quản lý mật khẩu ra đời.

- Một lưu ý nhỏ là người dùng vẫn cần ghi nhớ một mật khẩu chính duy nhất để mở khóa tất cả các mật khẩu khác. Do vậy, hãy đảm bảo rằng mật khẩu chính là mạnh nhất có thể (dưới đây sẽ có các hướng dẫn cụ thể).

- Thực tế, trình duyệt như Chrome và Firefox cũng có trình quản lý mật khẩu. Tuy nhiên, trang tin TechRepublic lại bày tỏ sự lo ngại về cách các trình duyệt này đảm bảo an toàn cho những mật khẩu lưu trữ và khuyến khích sử dụng ứng dụng chuyên dụng thay thế.

Hướng dẫn sử dụng trình quản lý mật khẩu trên Chrome

Cách xem, xóa hoặc xuất các mật khẩu đã lưu trên Chrome

1. Trên máy tính

Vào biểu tượng 3 chấm dọc góc trên cùng bên phải > Cài đặt > Mật khẩu > Nhập mật khẩu máy tính:

- Xem: Chọn vào icon mắt để xem mật khẩu.

- Xóa: Ở bên phải của trang web, hãy nhấp vào biểu tượng 3 chấm > Chọn Xóa.

- Xuất: Ở bên phải của mục Mật khẩu đã lưu, hãy nhấp vào biểu tượng 3 chấm > Chọn Xuất mật khẩu.

2. Trên điện thoại

- Mở ứng dụng Chrome > Chọn biểu tượng 3 chấm > Chọn Cài đặt > Chọn Mật khẩu.

- Xem: Nhấn vào biểu tượng mắt, nhập mật khẩu điện thoại nếu có.

- Xóa: Nhấn vào mật khẩu bạn muốn xóa. Ở trên cùng, hãy nhấn vào biểu tượng Xóa.

- Xuất: Nhấn vào biểu tượng 3 chấm > Chọn Xuất mật khẩu.

Cách kiểm tra, thay đổi mật khẩu đã lưu

1. Trên điện thoại

Mở ứng dụng Chrome > Nhấn vào biểu tượng 3 chấm > Chọn cài đặt > Chọn Đồng bộ hóa và các dịch vụ của Google > Bật hoặc tắt tính năng tùy chọn Cảnh báo bạn nếu mật khẩu bị lộ trong một sự cố rò rỉ dữ liệu.

2. Trên máy tính

Vào biểu tượng 3 chấm dọc góc trên cùng bên phải > Cài đặt > Chọn Mật khẩu > Chọn kiểm tra mật khẩu.

Hướng dẫn sử dụng trình quản lý mật khẩu trên Firefox

1. Hướng dẫn xem và xóa mật khẩu đã lưu trên Firefox

Chọn Cài đặt > Chọn Riêng tư và bảo mật > Kéo xuống phần Đăng nhập & mật khẩu > Chọn Đăng nhập đã lưu > Chọn biểu tượng hình con mắt để xem mật khẩu > Chọn Xóa nếu muốn xóa mật khẩu.

Quy tắc 2: Ghi thông tin đăng nhập ra giấy

- Đề xuất này trông có vẻ như đi ngược lại với những gì được nghe về bảo mật trực tuyến. Tuy nhiên, không phải ai cũng muốn sử dụng trình quản lý mật khẩu. Ngay cả những chuyên gia bảo mật hàng đầu như tổ chức quốc tế bảo vệ quyền lợi số (Electronic Frontier Foundation - EFF) đã khuyến cáo rằng, giữ thông tin đăng nhập trên giấy hoặc sổ ghi chú là một cách hữu hiệu để theo dõi thông tin đăng nhập.

- Lưu ý, giấy được nhắc đến là giấy thực sự theo cách truyền thống, không phải tài liệu điện tử như tệp Word hay bảng tính Google, bởi vì nếu một ai đó truy cập máy tính hay tài khoản online của người dùng, họ cũng có thể truy cập các file điện tử ghi thông tin mật khẩu.

- Tất nhiên, cũng có thể có người đột nhập và lấy được mật khẩu ghi trên giấy, nhưng điều này thường ít xảy ra hơn. Ở công ty hay ở nhà, cần giữ giấy ghi

mật khẩu ở nơi an toàn. Giới hạn số người biết nơi để giấy ghi mật khẩu, đặc biệt là thông tin đăng nhập các trang web tài chính.

- Nếu thường xuyên phải đi lại, việc mang theo giấy ghi mật khẩu sẽ mang lại rủi ro lớn nếu để nhầm hoặc đánh mất.

Quy tắc 3: Phát hiện mật khẩu đã bị rò rỉ hay chưa

- Người dùng khó có thể hoàn toàn ngăn chặn việc mật khẩu khỏi rò rỉ ra ngoài, có thể là qua sự cố rò rỉ thông tin, hoặc qua một tấn công độc hại. Nhưng người dùng có thể kiểm tra các dấu hiệu cho thấy tài khoản có thể bị xâm phạm bất cứ lúc nào.

- Công cụ Firefox Monitor của Mozilla và Password Checkup của Google có thể cho thấy địa chỉ email và mật khẩu nào của người dùng có thể bị xâm nhập trong các sự cố rò rỉ thông tin. Từ đó, người dùng biết khi nào cần có những biện pháp hành động thích hợp.

Quy tắc 4: Tránh những từ và tổ hợp ký tự phổ biến trong mật khẩu

- Mục đích trong việc tạo mật khẩu mạnh là để thiết lập một mật khẩu mà không ai khác có thể biết hoặc dễ dàng đoán được, như tránh xa các cụm từ phổ biến như "password", "mypassword" và các dãy kí tự dễ đoán như “qwerty” hay “thequickbrownfox”.

- Ngoài ra, tránh sử dụng tên, biệt danh của chính mình, tên thú cưng, ngày sinh hay ngày kỷ niệm, tên đường phố hay bất cứ thứ gì liên quan đến người dùng mà ai đó có thể tìm thấy từ phương tiện truyền thông, hay từ những cuộc trò chuyện giữa người dùng với một người lạ.

Quy tắc 5: Sử dụng ít 8 ký tự cho mật khẩu mạnh

- 8 ký tự là con số ít nhất để có thể tạo một mật khẩu mạnh, nhưng càng dài thì càng tốt. Tổ chức EFF cùng với chuyên gia bảo mật người Mỹ và nhiều chuyên gia khác, đã khuyến nghị người dùng sử dụng một cụm mật khẩu từ 3 hoặc 4 từ ngẫu nhiên nhằm tăng tính bảo mật. Tuy nhiên, cụm mật khẩu dài chứa các từ không có tính kết nối sẽ khiến khó nhớ. Đó là lý do mà người dùng nên xem xét sử dụng trình quản lý mật khẩu.

Quy tắc 6: Không tái sử dụng mật khẩu

- Cần luôn lưu ý rằng, việc tái sử sụng mật khẩu cho nhiều tài khoản khác nhau là một điều nguy hại. Nếu ai đó có được mật khẩu tái sử dụng trên một tài

khoản của người dùng, họ có thể sử dụng cho các tài khoản khác mà người dùng tái sử dụng mật khẩu đó.

- Việc sửa đổi mật khẩu gốc bằng cách thêm tiền tố hoặc hậu tố cũng sẽ dẫn đến mối đe dọa tương tự. Ví dụ như PasswordOne, PasswordTwo, cả hai mật khẩu này đều kém an toàn.

- Bằng cách sử dụng một mật khẩu riêng biệt với mỗi tài khoản, thì tin tặc có thể xâm nhập một tài khoản nhưng không thể sử dụng nó với những tài khoản còn lại của người dùng.

Quy tắc 7: Tránh sử dụng mật khẩu đã bị đánh cắp

Tin tặc có thể dễ dàng sử dụng các mật khẩu bị đánh cắp hoặc rò rỉ trước đó với công cụ tự động đăng nhập, được gọi là kỹ thuật nhồi thông tin đăng nhập (credential stuffing) để xâm nhập tài khoản.

Quy tắc 8: Không cần thiết lập lại mật khẩu theo định kỳ

- Nhiều năm qua, việc thay đổi mật khẩu sau 60 hoặc 90 ngày là một phương pháp được khuyến nghị rất nhiều, với lý do đây là thời gian cần thiết để mở khóa một mật khẩu.

- Tuy nhiên, hiện tại, Microsoft đã khuyến nghị rằng, người dùng không cần thay đổi mật khẩu định kỳ trừ khi nghi ngờ rằng mật khẩu có thể đã bị rò rỉ. Lý do là vì phần lớn người dùng, nếu bị bắt buộc phải thay đổi mật khẩu vài tháng một lần, sẽ dẫn đến thói quen nguy hiểm là tạo những mật khẩu dễ nhớ hoặc viết chúng lên giấy ghi chú và dính lên màn hình máy tính.

Quy tắc 9: Sử dụng xác thực 2 yếu tố (2FA) nhưng tránh mã tin nhắn văn bản

- Nếu tin tặc đánh cắp được mật khẩu, người dùng vẫn có thể ngăn chặn tin tặc chiếm quyền truy cập tài khoản bằng xác thực 2 yếu tố (cũng được gọi là xác minh hai bước hoặc 2FA). Đây là một biện pháp bảo mật an toàn, yêu cầu người dùng điền thông tin thứ 2 mà chỉ người dùng mới có (thường là mã dùng một lần) trước khi ứng dụng hoặc dịch vụ cho phép người dùng đăng nhập.

- Với biện pháp này, ngay cả khi tin tặc có được mật khẩu nhưng không có thiết bị tin tưởng của người dùng (như điện thoại) và mã xác minh để chứng thực rằng đó là người dùng, thì tin tặc sẽ không thể truy cập được vào tài khoản.

- Mặc dù, việc nhận mã bằng tin nhắn văn bản trên điện thoại di động hoặc bằng cách gọi điện trực tiếp trên điện thoại cố định là phổ biến và thuận tiện, thì việc tin tặc đánh cắp số điện thoại qua kỹ thuật gian lận trao đổi SIM (SIM swap fraud) là đơn giản, từ đó có thể chặn bắt mã xác nhận.

- Một cách an toàn hơn nhiều để nhận mã xác nhận là người dùng tự tạo và lấy chúng bằng cách dùng ứng dụng xác thực như Google Authentication hoặc Microsoft Authentiacator. Khi đã thiết lập xong, người dùng có thể chọn đăng ký thiết bị hoặc trình duyệt, từ đó người dùng không cần phải xác thực mỗi lần đăng nhập.

- Khi nói đến đảm bảo an toàn mật khẩu, thì sự chủ động bảo vệ của người dùng là biện pháp tốt nhất, trong đó cần biết được liệu email và mật khẩu của người dùng đã bị rò rỉ hay chưa./.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG