SANS SECURITY AWARENESS

# Hướng dẫn Thực hiện Nâng cao Nhận thức Bảo mật – Làm việc Bảo mật Tại nhà

# Phần Tóm tắt

Do dịch vi rút Corona, nhiều tổ chức đang chọn giải pháp chuyển nhân lực của mình sang làm việc tại nhà. Đây có thể là một thử thách vì nhiều tổ chức thiếu chính sách, công nghệ và chương trình đào tạo để đảm bảo an toàn cho nhân lực làm việc từ xa. Ngoài ra, nhiều nhân viên có thể thấy lạ lẫm hoặc không thoải mái với ý tưởng làm việc tại nhà. Mục đích của hướng dẫn này là nhằm giúp quý vị nhanh chóng đào tạo những nhân viên đó để đảm bảo an toàn nhất có thể. Nếu quý vị có câu hỏi nào về cách sử dụng hướng dẫn này, vui lòng liên hệ với chúng tôi theo địa chỉ support@sans.org.

Vì nhân lực của quý vị rất có khả năng sẽ gặp phải nhiều áp lực và thay đổi, còn tổ chức của quý vị thì rất có khả năng sẽ bị hạn chế bởi thời gian và nguồn lực, hướng dẫn chiến lược này sẽ tập trung vào thực hiện nội dung đào tạo đơn giản nhất có thể. Chúng tôi khuyến nghị quý vị chỉ tập trung vào các rủi ro quan trọng nhất, có tác động lớn nhất như được mô tả dưới đây. Hãy coi đây là điểm khởi đầu. Nếu có các rủi ro hay chủ đề khác mà quý vị muốn bổ sung, xin vui lòng thực hiện. Hãy nhớ rằng nếu quý vị yêu cầu nhân lực của mình thực hiện càng nhiều hành vi, quy trình và công nghệ thì khả năng họ thực hiện được tất cả các yêu cầu đó càng thấp.

# Cách Sử dụng Hướng dẫn Này

Chúng tôi khuyến nghị quý vị bắt đầu bằng cách đọc tài liệu trong hướng dẫn này và xem lại các liên kết dẫn đến các tài liệu khác nhau được cung cấp để nắm được tài nguyên nào đang có sẵn. Quý vị sẽ thấy rằng với mỗi rủi ro, chúng tôi đều cung cấp nhiều nội dung khác nhau mà quý vị có thể sử dụng để thu hút và đào tạo trong tổ chức của mình. Điều này cho phép quý vị chọn các mô hình mà quý vị thấy hoạt động hiệu quả nhất theo nhu cầu và văn hóa của tổ chức. Sau khi quý vị đọc xong tài liệu này, hãy đọc cả Mẫu Truyền đạt và Bảng Dữ liệu kèm theo bộ công cụ này để hiểu rõ thêm về mục tiêu mà quý vị đang cố gắng đạt được. Khi quý vị đã xem xong tài liệu, có hai nhóm chính mà quý vị cần điều phối với.

1. **Đội ngũ Bảo mật**: Điều phối với đội ngũ bảo mật của quý vị để hiểu rõ hơn về các rủi ro chính mà quý vị đang cố gắng quản lý. Trong hướng dẫn này, chúng tôi đã xác định những rủi ro mà chúng tôi coi là quan trọng nhất, phổ biến nhất đối với nhân lực làm việc tại nhà, nhưng rủi ro của quý vị có thể sẽ khác. Xin lưu ý rằng một sai lầm phổ biến mà đội ngũ bảo mật hay mắc phải là cố quản lý mọi rủi ro và khiến cho mọi người cảm thấy quá tải với quá nhiều chính sách và yêu cầu. Hãy cố gắng giới hạn các rủi ro mà quý vị sẽ đề cập ở mức thấp nhất có thể. Khi quý vị đã xác định được và ưu tiên các rủi ro này, hãy xác nhận các hành vi quản lý các rủi ro đó. Như đã đề cập, nếu tổ chức của quý vị không có thời gian hoặc tài nguyên cho nội dung này, hãy sử dụng nội dung mà chúng tôi trình bày bên dưới.

2. **Truyền thông**: Khi quý vị đã xác định được các rủi ro nhân lực hàng đầu và các hành vi chính để quản lý rủi ro, hãy hợp tác với đội ngũ truyền thông để thu hút và đào tạo nhân lực về các hành vi này. Các chương trình nâng cao nhận thức bảo mật hiệu quả nhất có mối quan hệ hợp tác chặt chẽ với các đội ngũ truyền thông của họ. Nếu có thể, hãy xem liệu quý vị có thể mời một số nhân viên của bộ phận truyền thông tham gia vào đội ngũ bảo mật của quý vị hay không. Khi giao tiếp với nhân lực của quý vị, quý vị có thể sử dụng một cách liên hệ hiệu quả để thu hút họ là nhấn mạnh rằng chương trình đào tạo này không chỉ giúp họ bảo mật tại nơi làm việc mà còn giúp họ tạo một ngôi nhà Bảo mật mạng, bảo vệ họ và gia đình của họ.

Sau cùng, nhờ vào sự phối hợp với hai nhóm này, quý vị đang cố biến bảo mật thành nội dung vừa đơn giản nhất có thể cho nhân sự của mình và vừa tạo động lực cho họ, là hai yếu tố chính để thay đổi hành vi. Chúng tôi đề xuất quý vị hãy thành lập một Ban cố vấn, bao gồm các thành viên chủ chốt để đưa ra phản hồi và ý kiến để quý vị triển khai chương trình. Ngoài đội ngũ bảo mật và truyền thông, thì Phòng Nhân sự và Phòng Pháp lý là các phòng ban khác quý vị nên hợp tác và phối hợp cùng.

## Gói Tải xuống Kỹ thuật số MGT433

SANS Institute cung cấp khóa đào tạo kéo dài hai ngày MGT433: Cách Xây dựng, Duy trì và Đo lường Chương trình Nâng cao Nhận thức Bảo mật Tác động lớn. Khóa đào tạo cường độ cao này cung cấp mọi lý thuyết, kỹ năng, bộ khung và tài nguyên để xây dựng một chương trình nâng cao nhận thức tác động cao để giúp quý vị quản lý hiệu quả và đo lường rủi ro về nhân lực của quý vị. Cũng trong hướng dẫn này, chúng tôi sẽ cung cấp quyền truy cập miễn phí Gói Tải xuống Kỹ thuật số của khóa học, có chứa các mẫu và tài nguyên lập kế hoạch. Mặc dù chúng rất có thể vượt quá nhu cầu của sáng kiến này, nhưng các nội dung này có thể rất hữu ích đối với những tổ chức lớn hơn hoặc chương trình triển khai phức tạp hơn.

## Giải đáp các câu hỏi về nhân lực

Ngoài hoạt động liên lạc với và đào tạo cho nhân lực của quý vị, chúng tôi đặc biệt khuyến nghị quý vị áp dụng công nghệ hoặc sử dụng diễn đàn để trả lời câu hỏi của mọi người, tốt nhất là theo thời gian thực. Chúng có thể bao gồm một biệt danh email dành riêng, kênh trò chuyện qua Skype hay Slack, hoặc một số loại hình diễn đàn trực tuyến như với Yammer. Một ý tưởng khác là tổ chức một chương trình truyền hình trực tiếp trên mạng, được quý vị lặp lại vài lần mỗi tuần để mọi người có thể chọn thời điểm phù hợp nhất với họ và tham dự sự kiện trực tiếp, thậm chí là để đặt câu hỏi. Mục tiêu là để quý vị đảm bảo rằng chủ đề bảo mật dễ tiếp cận nhất có thể cho mọi người và giúp giải đáp các câu hỏi của mọi người. Đây là một cơ hội tuyệt vời để gắn kết với nhân lực của quý vị và khiến bảo mật trở thành chủ đề gần gũi, hãy cố tận dụng cơ hội này. Xin lưu ý rằng, để điều này đạt được hiệu quả, quý vị nên dành riêng một nguồn lực để điều hành bất kỳ kênh bảo mật nào và tích cực trả lời các câu hỏi.

# Nội dung về Rủi ro & Đào tạo

Chúng tôi đã xác định ba rủi ro cốt lõi mà quý vị nên quản lý cho nhân lực làm việc từ xa của mình. Đây là điểm khởi đầu và rất có khả năng là những rủi ro có giá trị lớn nhất đối với quý vị. Mỗi rủi ro dưới đây đều có các liên kết đến nhiều nguồn tài nguyên để giúp truyền tải và đào tạo về chủ đề đó. Chúng tôi cung cấp nhiều tài liệu truyền đạt để quý vị có thể chọn những tài liệu có tác động lớn nhất cho môi trường của quý vị. Ngoài ra, hầu như tất cả các nội dung đều là tài liệu đa ngôn ngữ. Nếu toàn bộ nội dung này quá nhiều và quý vị có thời gian rất hạn chế, chúng tôi khuyến nghị quý vị chỉ sử dụng và triển khai hai nội dung được liệt kê bên dưới.

1. Bảng Dữ liệu về Làm việc An toàn Tại nhà (có trong Gói Triển khai của quý vị).
2. Video Tạo lập Ngôi nhà An toàn trên Không gian Mạng (tiếng Anh) cũng có sẵn qua các ngôn ngữ khác tại đây

## Kỹ thuật Xã hội

Một trong những rủi ro lớn nhất mà nhân viên làm việc từ xa phải đối mặt, đặc biệt là trong thời gian biến đổi khôn lường và môi trường cấp bách này là các cuộc tấn công kỹ thuật xã hội. Kỹ thuật Xã hội là một cuộc tấn công tâm lý, trong đó những kẻ tấn công lừa nạn nhân của chúng phạm phải sai lầm, và điều này được thực hiện dễ dàng hơn trong thời kỳ thay đổi và bối rối. Điều cốt lõi là đào tạo cho mọi người biết được kỹ thuật xã hội là gì, cách phát hiện các dấu hiệu phổ biến nhất của một cuộc tấn công kỹ thuật xã hội và điều cần làm khi phát hiện ra. Đảm bảo rằng quý vị không chỉ tập trung vào các cuộc tấn công lừa đảo qua email, mà cần tập trung vào các phương thức tấn công khác, bao gồm cuộc gọi điện thoại, nhắn tin, mạng xã hội hoặc tin giả. Quý vị có thể tìm nội dung mà quý vị cần để đào tạo và củng cố chủ đề này trong thư mục Nội dung Hỗ trợ Kỹ thuật Xã hội của chúng tôi. Ngoài ra, dưới đây là hai video Nâng cao Nhận thức Bảo mật của SANS mà quý vị có thể liên kết với, đây cũng là các video đa ngôn ngữ.

- Kỹ thuật Xã hội (tiếng Anh) cũng có trong các ngôn ngữ khác tại đây
- Lừa đảo (tiếng Anh) cũng có trong các ngôn ngữ khác tại đây

## Mật khẩu mạnh

Như được xác định trong DBIR thường niên của Verizon, mật khẩu yếu tiếp tục là một trong số những yếu tố chính gây ra các vụ xâm nhập trên phạm vi toàn cầu. Có bốn hành vi chính, được liệt kê bên dưới, để giúp quản lý rủi ro này. Quý vị có thể tìm thấy nội dung quý vị cần để đào tạo và củng cố cho chủ đề này và bốn hành vi chính này trong thư mục Mật khẩu của chúng tôi.

- Cụm từ mật khẩu (lưu ý là cả độ phức tạp của mật khẩu và hết hạn mật khẩu đều không hiệu quả).
- Mật khẩu riêng biệt cho mọi tài khoản
- Công cụ quản lý mật khẩu
- MFA (Xác thực đa yếu tố). Thường được gọi là Xác thực hai yếu tố hay Xác minh hai bước

## Các hệ thống được cập nhật

Rủi ro thứ ba là đảm bảo rằng bất kỳ công nghệ nào được nhân lực của quý vị sử dụng đều phải chạy phiên bản mới nhất của hệ điều hành, phần mềm và ứng dụng di động. Đối với những người sử dụng thiết bị cá nhân, điều này có thể yêu cầu bật tính năng tự động cập nhật. Quý vị có thể tìm nội dung cần thiết để đào tạo và củng cố chủ đề này trong thư mục Phần mềm Độc hại hoặc Tạo lập Ngôi nhà An toàn trên không gian Mạng.

### Các chủ đề khác cần cân nhắc

- **Wi-Fi**: Bảo mật điểm truy cập Wi-Fi của quý vị. Phần này được đề cập trong nội dung Tạo lập Ngôi nhà An toàn trên không gian Mạng. Ngoài ra, quý vị hãy cân nhắc xem video này trên Video Tạo lập Ngôi nhà An toàn trên không gian Mạng (tiếng Anh) cũng có trong các ngôn ngữ khác tại đây.

- **VPN**: VPN là gì và vì sao quý vị nên sử dụng. Chúng tôi khuyến nghị Thư tin của OUCH về VPN.

- **Làm việc Từ xa**: Đây là nội dung dành cho cá nhân, những người làm việc từ xa nhưng KHÔNG làm việc tại nhà, như làm việc tại quán cà phê, sân bay hoặc khách sạn. Hãy cân nhắc sử dụng nội dung Video đào tạo Làm việc Từ xa (tiếng Anh) cũng có trong các ngôn ngữ khác tại đây.

- **Trẻ em / Khách**: Để củng cố ý tưởng rằng gia đình / khách không nên truy cập các thiết bị liên quan đến công việc, hãy cân nhắc nội dung Video đào tạo Làm việc Từ xa (tiếng Anh) cũng có trong các ngôn ngữ khác tại đây.

- **Phát hiện / Phản ứng**: Quý vị có muốn người khác thông báo nếu họ cho rằng đã có một sự việc khi làm việc tại nhà không? Nếu có, quý vị muốn họ thông báo điều gì và khi nào? Chủ đề này được đề cập trong nội dung Bị hack của chúng tôi.

# Thư tin của OUCH

Ngoài ra, hãy cân nhắc sử dụng các thư tin công khai của OUCH để hỗ trợ chương trình của quý vị, mỗi thư tin đều được dịch sang hơn hai mươi ngôn ngữ. Được liệt kê ở bên dưới là các thư tin của OUCH mà chúng tôi thấy có thể hỗ trợ tốt nhất cho sáng kiến Làm việc Bảo mật tại Nhà của quý vị. Quý vị có thể tìm thấy toàn bộ thư tin tại mục Lưu trữ Thư tin Nâng cao Nhận thức Bảo mật của OUCH trực tuyến.

## TỔNG QUAN

Four Steps to Staying Secure (Bốn Bước để được Bảo mật)
https://www.sans.org/security-awareness-training/resources/four-simple-steps-staying-secure

Creating a Cybersecure Home (Tạo lập Ngôi nhà An toàn trên Không gian Mạng)
https://www.sans.org/security-awareness-training/ouch-newsletter/2018/creating-cybersecure-home

## KỸ THUẬT XÃ HỘI

Social Engineering (Kỹ thuật Xã hội)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/social-engineering

Messaging / Smishing (Gửi tin nhắn / Lừa đảo qua SMS)
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks

Personalized Scams (Lừa đảo được Cá nhân hóa)
https://www.sans.org/security-awareness-training/resources/personalized-scams

CEO Fraud (Giả mạo CEO)
https://www.sans.org/security-awareness-training/resources/ceo-fraudbec

Phone Call Attacks / Scams (Tấn công / Lừa đảo qua Điện thoại)
https://www.sans.org/security-awareness-training/resources/phone-call-attacks-scams

Stop That Phish (Ngăn chặn Lừa đảo)
https://www.sans.org/security-awareness-training/resources/stop-phish

Scamming You Through Social Media (Lừa đảo Quý vị Qua Mạng Xã hội)
https://www.sans.org/security-awareness-training/resources/scamming-you-through-social-media

## MẬT KHẨU

Making Passwords Simple (Tạo Mật khẩu Đơn giản)
https://www.sans.org/security-awareness-training/resources/making-passwords-simple

Lock Down Your Login (2FA) (Khóa chặt Thông tin Đăng nhập)
https://www.sans.org/security-awareness-training/ouch-newsletter/2017/lock-down-your-login

## CHỦ ĐỀ KHÁC

Yes, You Are a Target (Đúng, Quý vị Là Mục tiêu)
https://www.sans.org/security-awareness-training/resources/yes-you-are-target

Smart Home Devices (Thiết bị Ngôi nhà Thông minh)
https://www.sans.org/security-awareness-training/resources/smart-home-devices

# Lời khuyên Nhanh

Các mẹo và lời khuyên quý vị có thể chia sẽ dưới dạng dễ hiểu.

- Các bước hiệu quả nhất mà quý vị có thể áp dụng để bảo mật cho mạng không dây tại nhà là thay đổi mật khẩu quản trị viên mặc định, bật mã hóa WPA2 và sử dụng mật khẩu mạnh cho mạng không dây của mình.
- Hãy lưu ý tất cả các thiết bị được kết nối với mạng gia đình của quý vị, bao gồm thiết bị giám sát trẻ, máy chơi trò chơi, TV, thiết bị gia dụng hay thậm chí là xe hơi của quý vị. Đảm bảo rằng tất cả các thiết bị đó đều được bảo vệ bằng mật khẩu mạnh và/hoặc đang chạy phiên bản hệ điều hành mới nhất.
- Một trong số những cách hiệu quả nhất mà quý vị có thể bảo vệ máy tính của mình tại nhà là đảm bảo rằng cả hệ điều hành và ứng cụng của quý vị được vá lỗi và được cập nhật. Hãy bật chế độ cập nhật tự động bất cứ khi có thể.
- Sau cùng thì cảm nhận của bản thân là cách bảo vệ hiệu quả nhất của quý vị. Nếu email, cuộc gọi điện thoại hoặc tin nhắn trực tuyến có vẻ kỳ lạ, đáng ngờ, hoặc quá tốt so với lẽ thường, thì đó có thể là một cuộc tấn công.
- Đảm bảo rằng mỗi tài khoản của quý vị có một mật khẩu riêng biệt, duy nhất. Quý vị không thể nhớ hết được tất cả các mật khẩu/cụm từ mật khẩu của mình? Hãy cân nhắc sử dụng trình quản lý mật khẩu để lưu trữ bảo mật chúng cho quý vị.
- Xác minh hai bước là một trong những bước tốt nhất mà quý vị có thể áp dụng để bảo mật cho bất kỳ tài khoản nào. Xác minh hai bước là khi quý vị cần cả mật khẩu lẫn mã được gửi đến hoặc được tạo bởi thiết bị di động của quý vị. Các ví dụ về các dịch vụ hỗ

trợ xác minh hai bước gồm Gmail, Dropbox và Twitter.

- Lừa đảo là khi một kẻ tấn công cố lừa quý vị nhấn vào một liên kết độc hại hoặc mở một tệp đính kèm trong email. Hãy cảnh giác trước bất kỳ email hoặc tin nhắn trực tuyến tạo cảm giác cấp bách, có lỗi chính tả hoặc xưng hô với quý vị như "Khách hàng thân mến".

## Chỉ số đo lường

Chỉ số đo lường hành vi rất khó áp dụng cho tình huống này vì việc đo lường cách người khác cư xử tại nhà sẽ khó hơn rất nhiều. Ngoài ra, một vài hành vi trong số này không liên quan đến công việc (như bảo mật thiết bị Wi-Fi của họ). Tuy nhiên, quý vị có thể đo lường sự gắn kết. Chúng tôi thấy rằng các chủ đề cá nhân hay cảm xúc như vậy có thể rất lôi cuốn, thu hút sự quan tâm hơn rất nhiều các chủ đề khác. Do đó, các chỉ số đo lường như vậy có thể có giá trị.

- **Tương tác**: Mọi người đặt câu hỏi, đăng ý kiến hay yêu cầu trợ giúp trên các kênh bảo mật và diễn đàn mà quý vị đang điều hành ở mức độ nào?
- **Mô phỏng**: Thực hiện vài loại mô phỏng tấn công kỹ thuật xã hội, như lừa đảo, tấn công bằng tin nhắn hoặc cuộc gọi điện thoại.

Để biết danh sách chỉ số đo lường đầy đủ hơn, hãy tải xuống Bảng Chỉ số đo lường Nâng cao Nhận thức Bảo mật tương tác từ Gói Tải xuống Kỹ thuật số MGT433.

## Giấy phép



## Tác giả Bộ công cụ Triển khai

Lance Spitzner có hơn 20 năm kinh nghiệm về bảo mật trong lĩnh vực nghiên cứu mối đe dọa mạng, kiến trúc, nâng cao nhận thức và đào tạo về bảo mật. Ông đã hỗ trợ mở đường cho các lĩnh vực về thông tin lừa đảo và mạng thông qua việc sáng tạo ra kiến trúc honeynet và sáng lập Dự án Honeynet. Là một giảng viên tại SANS, ông đã phát triển các khóa MGT433: Nâng cao Nhận thức Bảo mật và MGT521: Văn hóa Bảo mật. Ngoài ra, Lance đã xuất bản ba cuốn sách về bảo mật, làm cố vấn tại hơn 25 quốc gia và hỗ trợ hơn 350 tổ chức xây dựng các chương trình nâng cao nhận thức và văn hóa bảo mật để quản lý rủi ro nhân sự của họ. Lance là một diễn giả nổi tiếng, thường xuyên đăng bài trên Twitter (@lspitzner) và tham gia vào nhiều dự án bảo mật cộng đồng. Trước khi làm việc trong lĩnh vực bảo mật thông tin, Ông Spitzne từng là một sĩ quan thiết giáp thuộc Lực lượng Triển khai nhanh của Quân đội và có bằng MBA tại trường Đại học Illinois.

## Thông tin về SANS Institute

SANS Institute được thành lập vào năm 1989 dưới hình thức một tổ chức nghiên và giáo dục hợp tác. SANS là tổ chức đáng tin cậy nhất và đến nay là nhà cung cấp lớn nhất về đào tạo bảo mật và cấp chứng nhận cho các chuyên gia tại các tổ chức chính phủ và thương mại trên khắp thế giới. Các giảng viên lừng danh tại SANS giảng dạy hơn 60 khóa học khác nhau tại hơn 200 sự kiện đào tạo bảo mật mạng trực tiếp cũng như trực tuyến. GIAC là một đơn vị liên kết của SANS Institute, phê chuẩn chứng chỉ hành nghề thông qua hơn 35 chứng nhận thực hành, kỹ thuật về bảo mật mạng. SANS Technology Institute, là một đơn vị chi nhánh độc lập, được công nhận theo khu vực, cấp bằng về bảo mật mạng. SANS cung cấp vô số tài nguyên miễn phí cho cộng đồng Bảo mật Thông tin, bao gồm các dự án chung, các báo cáo nghiên cứu, và thư tin; SANS cũng vận hành hệ thống cảnh báo sớm của Internet--hệ thống Internet Storm Center. SANS quy tụ nhiều chuyên gia về bảo mật, đại diện cho các tổ chức toàn cầu khác nhau từ các doanh nghiệp đến các trường đại học, hợp tác với nhau để hỗ trợ toàn bộ cộng đồng bảo mật thông tin. (https://www.sans.org)