Ưu tiên giáo dục và nâng cao nhận thức để vươn tới khả năng ứng phó phục hồi trên không gian mạng: Góc nhìn trực diện từ Việt Nam

Trong bài viết này, Vladimir Mariano, trưởng khoa công nghệ và đổi mới sáng tạo tại Học viện YSEALI thuộc Đại học Fulbright Việt Nam nhấn mạnh tầm quan trọng của giáo dục trong hành trình khả năng ứng phó phục hồi trên không gian mạng của Việt Nam

Bài viết này được xây dựng (viết ra) dựa trên nghiên cứu mới nhất của Tech For Food Institute (Viện nghiên cứu Công Nghệ vì cộng đồng) về khả năng phục hồi mạng.

Đọc nghiên cứu về khả năng ứng phó phục hồi mạng tại đây

Bởi Vladimir Mariano, PhD, trưởng khoa công nghệ và đổi mới sáng tạo, học viện YSEALI, Đại học Fulbright Việt Nam

Cũng như phần còn lại của khu vực Đông Nam Á, Việt Nam đang trải qua quá trình chuyển đổi kỹ thuật số cách nhanh chóng. Công nghệ và các mô hình kinh doanh dựa trên công nghệ được nhận định là bàn đạp cho sự tăng trưởng kinh tế. Việc sử dụng các công nghệ mới nổi, chẳng hạn như AI và blockchain, cũng đang rất phổ biến. Những công nghệ mới này được đón nhận tạo ra tiềm năng tác động tích cực cho đất nước.

Tuy nhiên, những rủi ro liên quan đến nền kinh tế số cũng càng ngày càng gia tăng. Chẳng hạn như blockchain được coi là trang mạng an toàn. Nhưng vào tháng 3 năm 2022 mạng Ronin của

Axie Infinity bị hack vẫn khiến người dùng tại Việt Nam bị ám ảnh. Ngoài ra còn có các sự cố an ninh mạng gần đây như Vietnamworks, Athena (công ty an ninh mạng) và hai sân bay lớn bị tin tặc tấn công.

Khi các mối đe doạ tiếp tục phát triển, điều quan trọng là Việt Nam cũng phải phát triển năng lực bảo vệ, xác định, phát hiện, ứng phó, phục hồi và thích ứng với các mối đe dọa mạng. Mặc dù vấn đề này có thể được giải quyết từ nhiều góc độ khác nhau nhưng giáo dục và xây dựng nhận thức là một khía cạnh nền tảng mà đất nước có thể ưu tiên.

Dự kiến nền kinh tế kỹ thuật số của Việt Nam sẽ tiếp tục tăng trưởng lên khoảng 49 tỷ USD vào năm 2030. Điều này có nghĩa là sẽ có nhiều người được tiếp cận với các giải pháp kỹ thuật số hơn và sẽ tham gia vào hệ sinh thái kỹ thuật số. Tuy nhiên, cũng sẽ có những người dùng lần đầu tiên lên mạng mà không hề biết đến những rủi ro cố hữu trong nền kinh tế số. Để duy trì sự tăng trưởng bền vững, điều quan trọng là phải duy trì niềm tin của người dùng vào các giải pháp kỹ thuật số thông qua trải nghiệm kỹ thuật số an toàn và bảo mật.

Bước đệm đầu tiên hướng tới việc thúc đẩy một xã hội kỹ thuật số tự tin là có các chiến dịch nâng cao nhận thức và xoá mù chữ trên mạng. Các chiến dịch này có thể bắt đầu từ các trường học và đại học, với trọng tâm là cho phép sử dụng internet hiệu quả hơn đồng thời giảm thiểu rủi ro mạng.

Các cơ sở giáo dục (mầm non, tiểu học và trung học) có thể bắt đầu đưa giáo dục an ninh mạng vào chương trình giảng dạy K-12 của Việt Nam. Đối với trẻ em, bao gồm những em được gọi là ' dân bản địa kỹ thuật số', cần được tiếp xúc sớm với vệ sinh mạng cơ bản (có nghĩa là giữ cho máy tính và mạng của bạn an toàn, được cập nhật để tin tặc khó có thể truy cập hay kiểm soát.) Các trường học nên tích cực thảo luận về lợi ích và rủi ro của các công nghệ mới nổi như blockchain, dịch vụ tài chính, trình chỉnh sửa video thông minh, nhân bản giọng nói và AI tổng hợp. Điều này sẽ cho phép sinh viên sử dụng các công nghệ này một cách có trách nhiệm hơn.

Năm 2021, các trường trung học ở Việt Nam bắt đầu tích hợp an ninh mạng vào chương trình giảng dạy của mình. Dựa trên sáng kiến này, có cơ hội để thấm nhuần văn hóa ứng phó trong giới trẻ. Điều này đòi hỏi phải thay đổi tư duy, chuẩn bị bản thân cho các tình huống không thể tránh khỏi như bị tấn công mạng và học cách thích ứng để giảm thiểu tác động của các mối đe dọa đó. Để đạt được điều này, các trường học nên cân nhắc việc thành lập các phòng thí nghiệm về khả năng ứng phó phục hồi mạng, cung cấp một môi trường an toàn nơi học sinh có thể trải nghiệm các bài tập trên bàn, tham gia diễn tập mạng và tham gia các cuộc thi an ninh mạng. Ngoài ra, các phòng thí nghiệm này có thể đóng vai trò là nền tảng để sinh viên tìm hiểu cách xác định và chống lại thông tin sai lệch cũng như các thông tin xuyên tạc thông qua các hoạt động tương tác như Trò Chơi Tin Giả (the Bad News Game)

Ngoài việc trang bị cho sinh viên những kỹ năng an ninh mạng cơ bản, các trường học và trường đại học cũng sẽ là nơi cung ứng lực lượng lao động trong lĩnh vực an ninh mạng đang bị thiếu hụt. Từ nghiên cứu về Khả năng ứng phó phục hồi mạng của Viện Tech For Good, Việt Nam có 76 chuyên gia được CISSP chứng nhận vào năm 2021, xếp cuối cùng trong số các quốc gia SEA-6. Thông qua các chiến dịch giáo dục và nâng cao nhận thức trong các trường học và đại học, các thế hệ sau những lực lượng lao động kỹ thuật số trong tương lai sẽ được giới thiệu về những công việc (nghề nghiệp) liên quan đến lĩnh vực an ninh mạng. Mặc dù mục tiêu là truyền cảm hứng để thu hút thêm nhiều sinh viên tham gia các ngành nghề liên quan đến an ninh mạng, nhưng sẽ có lợi cho Việt Nam nếu sinh viên mới tốt nghiệp có hiểu biết cơ bản về an ninh mạng, bất kể lĩnh vực chuyên môn của họ là gì.

Cuối cùng, để tạo ra một không gian mạng linh hoạt, cần có chỗ cho sự hợp tác giữa giới học thuật và khu vực tư nhân ở Việt Nam. Không thể phủ nhận rằng công nghệ đang phát triển với tốc độ chóng mặt và có thể khiến một số khái niệm hoặc kỹ năng được học ở trường trở nên lỗi thời. Các trường đại học có thể hưởng lợi từ sự hợp tác với các chuyên gia trong ngành để duy trì các chương trình và chương trình giảng dạy của họ luôn cập nhật. Điều này cũng sẽ cho phép các trường đại học đào tạo ra những sinh viên tốt nghiệp có kỹ năng phù hợp, phù hợp với nhu cầu của các ngành công nghiệp. Khu vực tư nhân cũng có thể cân nhắc việc học nghề trên mạng để cung cấp cho sinh viên trải nghiệm và đào tạo thực tế về an ninh mạng.

Vladimir Mariano, PhD là Trưởng khoa Công nghệ và Đổi mới sáng tạo tại Học viện YSEALI thuộc Đại học Fulbright Việt Nam. Ông đã lãnh đạo Học viện YSEALI trong việc thiết kế và thực hiện hai hội thảo lãnh đạo có tựa đề "Số hóa niềm tin" và "AI sáng tạo và ảnh hưởng văn hóa", thảo luận về ý nghĩa xã hội, đạo đức và pháp lý của các công nghệ như tác nhân AI, blockchain, deepfake và AI tổng quát. Tốt nghiệp ngành Khoa học Máy tính tại Penn State, Tiến sĩ Mariano đã phục vụ trong giới học thuật và công nghiệp tại Hoa Kỳ, Philippines và Việt Nam.

Các quan điểm và đề xuất được trình bày trong bài viết này chỉ thuộc về/các tác giả và không nhất thiết phản ánh quan điểm cũng như lập trường của Tech for Good Institute.

—----------

LinkedIn Blurb:

Việt Nam, cũng như phần còn lại của Đông Nam Á, đang trong quá trình chuyển đổi kỹ thuật số nhanh chóng. Tuy nhiên, tiến trình này đi kèm với rủi ro gia tăng trong nền kinh tế kỹ thuật số. Bất chấp nhận thức về blockchain là một mạng an toàn, vụ hack Ronin Network trên Axie Infinity vào tháng 3 năm 2022 vẫn còn là mối lo ngại đối với người dùng tại Việt Nam.

Khi các mối đe dọa trong bối cảnh kỹ thuật số tiếp tục phát triển, điều quan trọng là Việt Nam phải phát triển năng lực bảo vệ, xác định, phát hiện, ứng phó, phục hồi và thích ứng với các mối đe dọa mạng.

Trong bài viết này, Vladimir Mariano, PhD, Trưởng khoa Công nghệ và Đổi mới, Học viện YSEALI, Đại học Fulbright Việt Nam, đi sâu vào những lỗ hổng và thách thức mà Việt Nam gặp phải khi giải quyết các mối đe dọa an ninh mạng.

Đọc thêm tại đây (read more here)