



EBOOK

BÌNH DÂN HỌC VỤ SỐ

SỐ 10/2025

CHUYÊN ĐỀ
AN TOÀN TRÊN KHÔNG GIAN MẠNG



MỤC LỤC

I. KIẾN THỨC, KỸ NĂNG SỐ CƠ BẢN

1. Tổng quan về không gian mạng, an toàn thông tin mạng.....	3
2. Nhận diện tấn công lừa đảo trên không gian mạng.....	6
3. Hướng dẫn thay đổi mật khẩu và passcode trên VneID.....	8
4. Hướng dẫn cập nhật phần mềm trên điện thoại thông minh.....	9
5. Hướng dẫn sao lưu dữ liệu trên điện thoại thông minh.....	10
6. Hướng dẫn cách cấp quyền truy cập cho ứng dụng trên điện thoại thông minh.....	11
7. Hướng dẫn tắt theo dõi quảng cáo Google Chrome trên điện thoại thông minh.....	13
8. Cảnh báo chiêu lừa đảo mới khai thác tính năng Find My của Apple.....	14
9. Một số lưu ý khi sử dụng Wifi công cộng.....	15

II. TRAO ĐỔI THẢO LUẬN

1. Dự báo các mối đe dọa và thách thức an ninh mạng năm 2025.....	16
2. Công ước Hà Nội: Dấu mốc lịch sử kiến tạo trật tự pháp lý toàn cầu về an ninh mạng.....	20
3. AI đang khuếch đại nguy cơ tấn công mạng thế nào.....	24
4. Lừa đảo mua sắm trực tuyến tăng cao vào dịp cuối năm.....	27
5. Nâng cao kỹ năng bảo đảm an ninh, an toàn trên không gian mạng của sinh viên các trường đại học, cao đẳng hiện nay.....	29
6. Ra mắt “Hệ thống điều hành an ninh mạng Quốc gia”.....	32

III. HỎI ĐÁP

1. Các nguy cơ mất an toàn phổ biến mà người dùng cần cảnh giác khi tham gia môi trường mạng là gì?	34
2. Cần làm gì để tự bảo vệ mình trước các mối nguy hại trên không gian mạng?.....	35
3. Những thói quen tốt giúp duy trì an toàn trên không gian mạng lâu dài?...36	
4. Cách xử lý khi vô tình nhấp vào một liên kết độc hại hoặc nghi ngờ độc hại?.....	38
5. Xác thực đa yếu tố (MFA) có quan trọng không?.....	39

TỔNG QUAN VỀ KHÔNG GIAN MẠNG, AN TOÀN THÔNG TIN MẠNG

Không gian mạng là gì?

Theo Khoản 3, Điều 2 của Luật An ninh mạng 2018 thông qua ngày 12/6/2018 có hiệu lực thi hành từ 01/01/2019, không gian mạng là hệ thống kết nối các nền tảng công nghệ thông tin, bao gồm mạng Internet, mạng viễn thông, mạng máy tính, hệ thống thông tin và các cơ sở dữ liệu. Đây là môi trường nơi con người có thể thực hiện các hoạt động giao tiếp, trao đổi thông tin, kinh doanh và giải trí mà không bị giới hạn bởi khoảng cách địa lý hay thời gian.



Sự phát triển của không gian mạng giúp con người dễ dàng kết nối, tìm kiếm thông tin và thực hiện các hoạt động kinh doanh, học tập trực tuyến, ...

Khác với không gian vật lý ba chiều trong thế giới thực, không gian mạng được xem là một không gian ảo, nơi mọi hoạt động số hóa diễn ra mà không cần đến sự tương tác trực tiếp giữa con người với nhau. Không gian mạng rất rộng lớn và bao gồm nhiều nền tảng, dịch vụ khác nhau, có thể chia thành các nhóm chính như:

- *Trình duyệt web*: Bao gồm các công cụ giúp truy cập Internet như Google Chrome, Mozilla Firefox, Safari, ...
- *Trang tin tức trực tuyến*: Là các nền tảng cung cấp thông tin thời sự, giải trí như VnExpress, Zing News, VTC News, ...
- *Mạng xã hội*: Là những nền tảng kết nối người dùng như Facebook, Twitter, Instagram, YouTube, ...
- *Dịch vụ trực tuyến*: Là các hệ thống hỗ trợ giao dịch, mua sắm, học tập, giải trí như chuyển tiền điện tử, tuyển dụng việc làm, thương mại điện tử, nghe nhạc trực tuyến, ...

Đặc điểm của không gian mạng Việt Nam

Không gian mạng tại Việt Nam đang phát triển mạnh mẽ, tạo ra nhiều cơ hội cho các hoạt động kinh tế, giáo dục và giải trí trực tuyến

Về mặt kỹ thuật, không gian mạng được xây dựng trên 3 lớp chính:

- *Hạ tầng truyền dẫn*: Bao gồm các thiết bị phần cứng như máy chủ, hệ thống mạng, trung tâm dữ liệu...
- *Dịch vụ lõi*: Tập hợp các giao thức, phần mềm hệ thống, nền tảng công nghệ giúp truyền tải, xử lý và bảo mật thông tin.
- *Hệ thống ứng dụng*: Các phần mềm, cơ sở dữ liệu phục vụ nhu cầu lưu trữ, trao đổi và khai thác thông tin.

Về mặt xã hội, không gian mạng không chỉ là một hệ thống công nghệ mà còn là môi trường giao tiếp và tương tác trực tuyến với 6 yếu tố quan trọng:

- Chính sách, pháp luật về an toàn thông tin
- Trình độ công nghệ và cơ sở hạ tầng
- Nội dung số và dữ liệu trực tuyến
- Đội ngũ nhân lực chuyên môn trong lĩnh vực công nghệ
- Cách tổ chức và quản lý các nền tảng mạng
- Ý thức và hành vi của người dùng khi tham gia không gian mạng

An toàn thông tin mạng là gì?

Theo khoản 1 điều 3 Luật An toàn thông tin mạng 2015 an toàn thông tin mạng là sự bảo vệ thông tin và hệ thống thông tin trên mạng tránh bị những tác động tiêu cực từ bên ngoài nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

Việc bảo đảm an toàn thông tin mạng cần tuân theo những nguyên tắc sau:

- Cơ quan, tổ chức, cá nhân có trách nhiệm bảo đảm an toàn thông tin mạng. Hoạt động an toàn thông tin mạng của cơ quan, tổ chức, cá nhân phải đúng quy định của pháp luật, bảo đảm quốc phòng, an ninh quốc gia, bí mật nhà nước, giữ vững ổn định chính trị, trật tự, an toàn xã hội và thúc đẩy phát triển kinh tế xã hội.

- Tổ chức, cá nhân không được xâm phạm an toàn thông tin mạng của tổ chức, cá nhân khác.
- Việc xử lý sự cố an toàn thông tin mạng phải bảo đảm quyền và lợi ích hợp pháp của tổ chức, cá nhân, không xâm phạm đến đời sống riêng tư, bí mật cá nhân, bí mật gia đình của cá nhân, thông tin riêng của tổ chức.
- Hoạt động an toàn thông tin mạng phải được thực hiện thường xuyên, liên tục, kịp thời và hiệu quả.



An toàn thông tin mạng là sự bảo vệ thông tin và hệ thống thông tin trên mạng tránh bị những tác động tiêu cực từ bên ngoài nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin.

Tại Điều 21 Luật An toàn thông tin mạng 2015 quy định về phân loại cấp độ an toàn hệ thống thông tin mạng như sau:

- Cấp độ 1 là cấp độ mà khi bị phá hoại sẽ làm tổn hại tới quyền và lợi ích hợp pháp của tổ chức, cá nhân nhưng không làm tổn hại tới lợi ích công cộng, trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;
- Cấp độ 2 là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc làm tổn hại tới lợi ích công cộng nhưng không làm tổn hại tới trật tự, an toàn xã hội, quốc phòng, an ninh quốc gia;
- Cấp độ 3 là cấp độ mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, an ninh quốc gia;
- Cấp độ 4 là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại nghiêm trọng tới quốc phòng, an ninh quốc gia;
- Cấp độ 5 là cấp độ mà khi bị phá hoại sẽ làm tổn hại đặc biệt nghiêm trọng tới quốc phòng, an ninh quốc gia.

Việc phân loại cấp độ an toàn hệ thống thông tin là để áp dụng biện pháp quản lý và kỹ thuật nhằm bảo vệ hệ thống thông tin phù hợp theo cấp độ./.

Trần Song (t/h)

NHẬN DIỆN TẤN CÔNG LỪA ĐẢO TRÊN KHÔNG GIAN MẠNG

Một số thủ đoạn lừa đảo mới trên không gian mạng thời gian gần đây:

1. Các đối tượng lừa đảo tìm kiếm, thu thập thông tin cá nhân (số điện thoại, tài khoản mạng xã hội, hình ảnh) sau đó sử dụng công nghệ trí tuệ nhân tạo (AI) cắt ghép hình ảnh của người dân/quân nhân (gọi tắt là nạn nhân) vào các hình ảnh, video nhạy cảm... rồi nhắn tin, gọi điện uy hiếp, yêu cầu chuyển tiền nhằm chiếm đoạt tài sản.

2. Làm nhiệm vụ “việc nhẹ, lương cao” qua mạng để nhận hoa hồng: Các đối tượng tiếp cận tài khoản mạng xã hội của nạn nhân, mời gọi tham gia làm nhiệm vụ online với cam kết thu nhập cao. Khi đồng ý tham gia, nạn nhân có thể nhận được tiền lãi sau một số nhiệm vụ ban đầu với số tiền nhỏ. Dần dần, chúng sẽ yêu cầu nạn nhân đầu tư số tiền lớn hơn hoặc lấy nhiều lý do để “giam tiền” như: Cơ quan thuế nước ngoài phong tỏa, thao tác sai, lỗi giao dịch... và yêu cầu nạn nhân chuyển thêm tiền để có thể rút toàn bộ vốn về. Sau khi đạt được mục đích, các đối tượng cắt đứt liên lạc.

3. Lừa nạn nhân truy cập vào đường link giả mạo để chiếm đoạt tài khoản mạng xã hội: Các đối tượng giả làm “hotgirl”, bạn bè... kết bạn online với nạn nhân, dẫn dụ nạn nhân truy cập vào các đường link có giao diện giống mạng xã hội (Facebook, Zalo...) do chúng tạo dựng. Khi nạn nhân đăng nhập tài khoản mạng xã hội sẽ bị chúng thu thập tài khoản, mật khẩu. Khi chiếm được quyền điều khiển tài khoản mạng xã hội của nạn nhân, các đối tượng sẽ nhắn tin, gọi điện đánh lừa người thân, quen của nạn nhân vay, mượn tiền nhằm chiếm đoạt tài sản.



Người dân cần cảnh giác với các thủ đoạn lừa đảo trên không gian mạng

4. Các đối tượng giả danh cơ quan chức năng (công an, tòa án, viện kiểm sát...) gọi điện hoặc nhắn tin thông báo nạn nhân có liên quan đến vụ việc nào đó để đe dọa. Thông thường, các đối tượng yêu cầu nạn nhân gọi video trực tuyến, thậm chí tạo dựng không gian làm việc giống trụ sở cơ quan công quyền nhằm lấy niềm tin. Tiếp đó, chúng sẽ gửi link cài ứng dụng, phần mềm chứa mã độc. Các ứng dụng, phần mềm này hoạt động ngầm, đánh cắp mã OTP, thông tin đăng nhập, mật khẩu và chuyển tiền khỏi tài khoản của nạn nhân.

5. Giả mạo nhân viên công ty điện lực, công ty nước sạch... để lừa đảo. Hình thức này tuy không mới, nhưng vẫn có nhiều người trở thành nạn nhân.

Các đối tượng thường giả danh nhân viên công ty điện lực, nước sạch... gọi điện hoặc nhắn tin với nạn nhân thông báo khách hàng nợ tiền điện, nước hoặc sử dụng dịch vụ bất thường, đe dọa nếu không thanh toán ngay sẽ bị ngừng cung cấp dịch vụ. Tiếp đó, các đối tượng đề nghị khách hàng kết bạn qua ứng dụng nhắn tin (Zalo, Viber...), hướng dẫn tải ứng dụng giả mạo của công ty điện lực, công ty nước sạch hoặc gửi mã QR yêu cầu nạn nhân thanh toán qua các kênh đó. Khi nạn nhân truy cập vào đường link tải ứng dụng giả mạo hoặc quét mã QR thì sẽ bị các đối tượng chiếm quyền điều khiển thiết bị và dễ dàng chiếm đoạt số tiền trong tài khoản ngân hàng.

6. Lừa đảo các gói du lịch nghỉ hè hấp dẫn: Thủ đoạn lừa đảo này lợi dụng nhu cầu săn vé máy bay giá rẻ và voucher (khuyến mại) du lịch của người dân. Các đối tượng lập các hội nhóm bán vé máy bay, thanh lý voucher du lịch, quảng cáo các gói khuyến mãi, giảm giá tour du lịch tại các khu nghỉ dưỡng nổi tiếng. Khi khách hàng liên hệ, chúng yêu cầu chuyển khoản đặt cọc một phần tiền. Sau khi nhận tiền, trang web hoặc hội nhóm kể trên sẽ biến mất.

7. Kêu gọi đầu tư tài chính, tiền ảo với lợi nhuận cao: Các đối tượng lừa đảo lập các website và ứng dụng đầu tư tài chính giả mạo, hứa hẹn lãi suất cao và khả năng rút vốn dễ dàng. Ban đầu, chúng trả lãi đầy đủ để tạo lòng tin từ nạn nhân. Tuy nhiên, khi nạn nhân tiếp tục đầu tư với số tiền lớn hơn, các đối tượng lập tức chặn tài khoản và chiếm đoạt toàn bộ số tiền.



Cán bộ, chiến sĩ Bộ tư lệnh 86 tham gia diễn tập về an toàn thông tin, bảo vệ chủ quyền quốc gia trên không gian mạng. Ảnh: Anh Thế

8. Mạo danh dịch vụ hỗ trợ lấy lại tiền đã bị lừa: Đánh vào tâm lý hoang mang của những người vừa bị lừa đảo qua mạng, các đối tượng đóng vai luật sư, nhân viên ngân hàng, kỹ sư công nghệ thông tin... quảng cáo có thể giúp những người từng bị lừa đảo lấy lại tiền đã mất. Chúng liên tục gọi điện, nhắn tin và yêu cầu nạn nhân phải trả trước “phí dịch vụ”. Sau khi thu được tiền từ nạn nhân, các đối tượng lập tức cắt đứt liên lạc./.

Tường Vy

HƯỚNG DẪN THAY ĐỔI MẬT KHẨU VÀ PASSCODE TRÊN VNEID



Để bảo mật tài khoản cũng như các thông tin cá nhân trên VNeID, cần thay đổi mật khẩu và passcode tài khoản định kỳ

Bước 1: Mở ứng dụng VNeID và đăng nhập vào tài khoản.

Trước tiên, cần mở ứng dụng VNeID trên điện thoại và đăng nhập vào tài khoản bằng mật khẩu hiện tại.

Bước 2: Truy cập vào phần “Cài đặt”.

Bước 3: Chọn mục “Đổi mật khẩu”.

Trong mục Cài đặt, tìm “Đổi mật khẩu” để tiến hành thay đổi mật khẩu. Sau đó, nhập mật khẩu hiện tại để xác minh.

Bước 4: Nhập mật khẩu mới.

Khi xác minh mật khẩu hiện tại, sẽ được yêu cầu nhập mật khẩu mới. Mật khẩu mới cần đáp ứng các yêu cầu bảo mật, chẳng hạn như độ dài tối thiểu, kết hợp chữ cái và số, để tăng cường bảo mật cho tài khoản. Sau đó nhập lại mật khẩu mới một lần nữa để xác nhận.

Bước 5: Thay đổi passcode

Nếu muốn thay đổi passcode (mã số bảo mật 6 chữ số), vào mục “Đổi passcode” trong cùng phần Cài đặt, nhập passcode cũ và sau đó chọn một passcode mới mong muốn.

Bước 6: Xác nhận và lưu thay đổi

Sau khi thay đổi mật khẩu và passcode, cần xác nhận lại các thông tin và nhấn “Lưu” để hoàn tất quá trình thay đổi.

Thay đổi mật khẩu và passcode trên VNeID là một biện pháp quan trọng để bảo vệ thông tin cá nhân và tăng cường bảo mật cho tài khoản VNeID./.

HƯỚNG DẪN CẬP NHẬT PHẦN MỀM TRÊN ĐIỆN THOẠI THÔNG MINH

*** Đối với iPhone, iPad**

Bước 1: Vào Cài đặt, chọn Cài đặt chung.



Bước 2: Chọn Cập nhật phần mềm, chọn Tự động cập nhật.

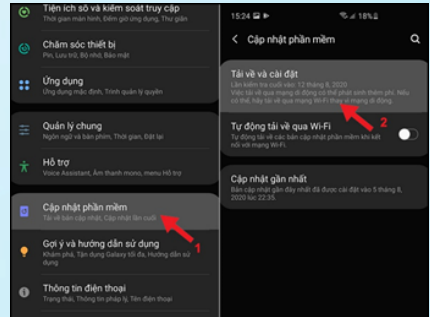


Bước 3: Có thể lựa chọn tự động tải về và cài đặt các bản cập nhật.



*** Đối với điện thoại Android**

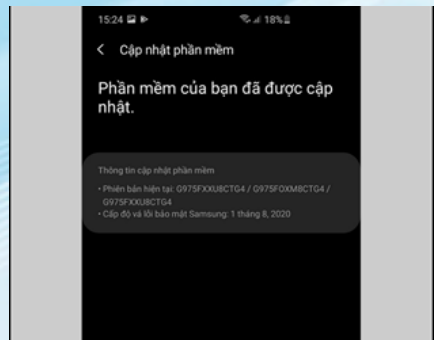
Mở Cài đặt rồi kéo xuống dưới, chọn Cập nhật phần mềm, chọn Tải về và cài đặt.



Lúc này, điện thoại sẽ:

+ Hiển thị thông tin phiên bản mới nhất (nếu có) để bạn quyết định xem có tải về hay không, sau khi tải xong máy sẽ hỏi bạn muốn nâng cấp ngay hay chọn thời gian khác (thường là buổi đêm). Hãy chọn thời gian phù hợp theo lịch biểu của bạn.

+ Đưa ra thông báo cho biết hệ thống của bạn là mới nhất (phần mềm của bạn đã được cập nhật), lúc này bạn chỉ việc thoát ra là xong.

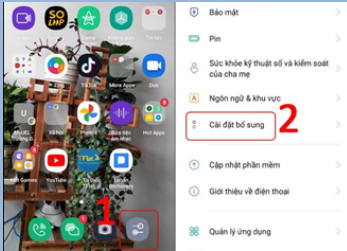


HƯỚNG DẪN SAO LƯU DỮ LIỆU TRÊN ĐIỆN THOẠI THÔNG MINH

Để đảm bảo an toàn cho dữ liệu và nếu chẳng may xảy ra trường hợp bị mất dữ liệu thì khôi phục được thì nên thực hiện sao lưu dữ liệu thường xuyên và sao lưu trước khi cập nhật phần mềm.

*** Cách sao lưu đối với điện thoại Android:**

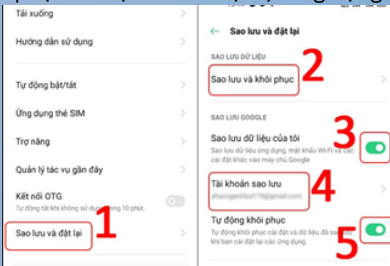
Bước 1: Vào Cài đặt, chọn Cài đặt bổ sung.



Bước 2: Chọn Sao lưu và đặt lại, chọn Sao lưu và khôi phục.

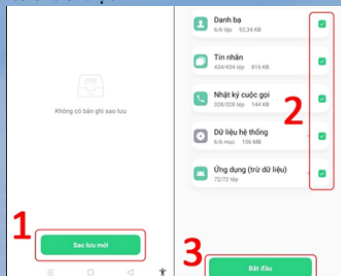
Nếu muốn tự động sao lưu từ Google thực hiện theo các bước tiếp theo:

- (3) Gạt nút sang phải ở mục Sao lưu dữ liệu của tôi.
- (4) Chọn tài khoản Google muốn sao lưu.
- (5) Gạt nút sang phải để chọn tự động sao lưu dữ liệu khi cài đặt lại ứng dụng.



Chọn Sao lưu và đặt lại, chọn Sao lưu và khôi phục

Bước 3: Chọn Sao lưu mới, chọn các mục cần sao lưu, chọn Bắt đầu và đợi thiết bị sao lưu dữ liệu.



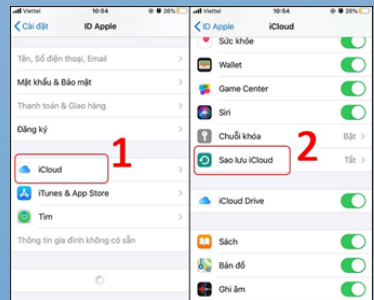
Chọn Bắt đầu và đợi thiết bị sao lưu dữ liệu

*** Cách sao lưu đối với iPhone, iPad:**

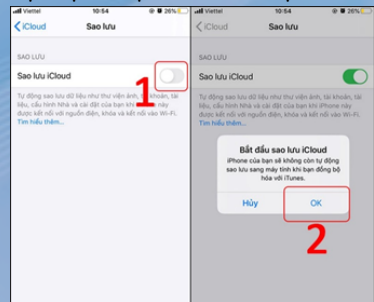
Bước 1: Chọn Cài đặt, chọn Ô có tên người dùng như hình minh họa.



Bước 2: Chọn iCloud, chọn Sao lưu iCloud.



Bước 3: Gạt nút sang phải, chọn OK và chờ đợi điện thoại sao lưu dữ liệu. Gạt nút sang phải, chọn OK và chờ đợi điện thoại sao lưu dữ liệu.



HƯỚNG DẪN CÁCH CẤP QUYỀN TRUY CẬP CHO ỨNG DỤNG TRÊN ĐIỆN THOẠI THÔNG MINH

Việc quản lý và cấp quyền truy cập cho ứng dụng trên điện thoại cần được lưu ý để tránh bị lạm dụng hoặc mất thông tin cá nhân cho một số ứng dụng độc hại, đồng thời nhắc nhở về việc tải các ứng dụng trên các nền tảng được cấp phép để đảm bảo an toàn cho thiết bị di động.

*** Đối với Android:**

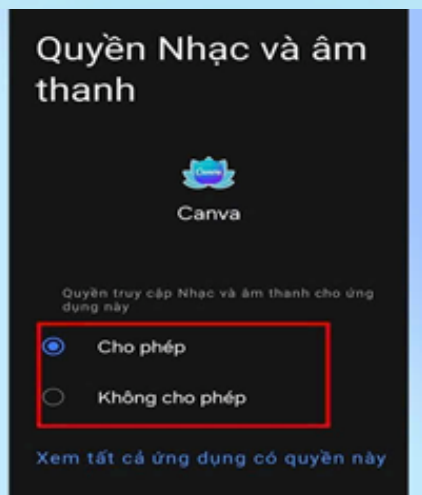
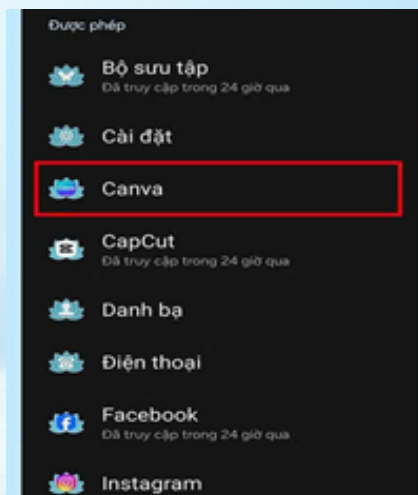
Bước 1: Vào Cài đặt, ấn chọn Ứng dụng.

Bước 2: Tại đây, ấn vào dấu 3 chấm ở góc trên bên phải màn hình Android và ấn Trình quản lý quyền.



Bước 3: Sau đó trong một quyền bất kỳ, ấn tìm ứng dụng cần cấp quyền.

Bước 4: Ấn vào Cho phép nếu muốn cấp quyền và Từ chối nếu không đồng ý quyền truy cập.



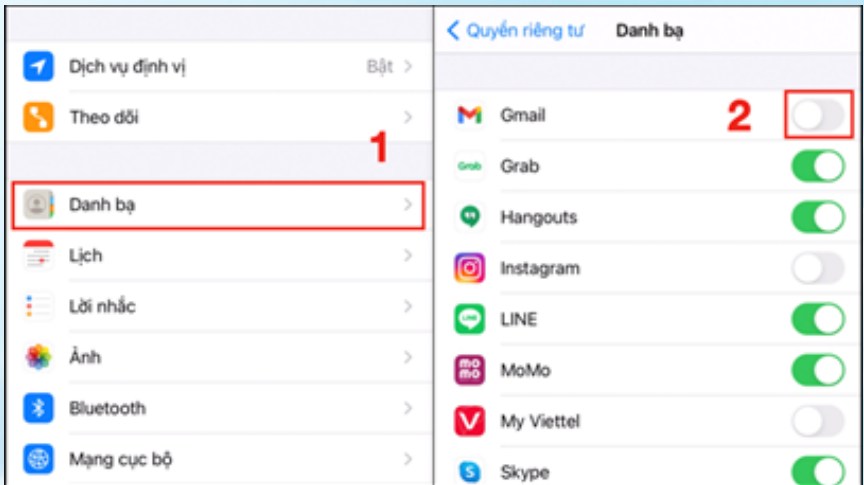
* Đối với iPhone:

Bước 1: Truy cập Cài đặt, nhấn chọn Quyền riêng tư.



Bước 2: Lựa chọn loại thông tin muốn kiểm tra quyền truy cập, nhấn bật/tắt quyền truy cập thông tin của ứng dụng.

Ví dụ ở đây là truy cập vào quyền cấp Danh bạ, sau đó tắt quyền truy cập cho ứng dụng Gmail.

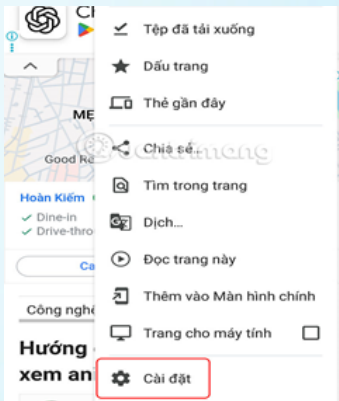


Tắt quyền truy cập Danh bạ cho Gmail.

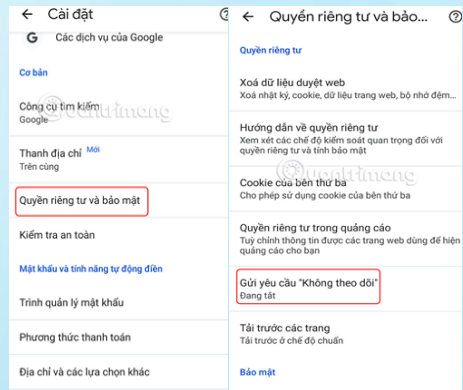
HƯỚNG DẪN TẮT THEO DÕI QUẢNG CÁO GOOGLE CHROME TRÊN ĐIỆN THOẠI THÔNG MINH

Theo dõi quảng cáo trong Google Chrome cho phép các trang web và nhà quảng cáo theo dõi hoạt động của người dùng. Dữ liệu này sau đó được sử dụng để cung cấp cho quảng cáo. Để bảo mật quyền riêng tư hơn, nên bật chế độ “không theo dõi” (Do Not Track). Khi đó tính năng này sẽ gửi tín hiệu ưu tiên quyền riêng tư đến các trang website, giảm thiểu tình trạng theo dõi không mong muốn. Dưới đây là hướng dẫn tắt theo dõi quảng cáo trên Google Chrome.

Bước 1: Tại giao diện Google Chrome trên điện thoại nhấn vào biểu tượng 3 chấm rồi chọn Cài đặt trong danh sách hiển thị.



Bước 2: Chuyển vào giao diện các thiết lập cho trình duyệt Chrome, nhấn chọn tiếp vào Quyền riêng tư và bảo mật. Nhấn vào thiết lập Gửi yêu cầu “Không theo dõi”.



Bước 3: Mặc định tính năng này đang tắt nên cần bật tính năng Không theo dõi trên Google Chrome để tăng cường bảo mật quyền riêng tư.



CẢNH BÁO CHIÊU LỪA ĐẢO MỚI KHAI THÁC TÍNH NĂNG FIND MY CỦA APPLE

Mới đây, các chuyên gia an ninh mạng cảnh báo về chiêu thức lừa đảo tinh vi nhắm vào người dùng iPhone bị mất máy. Kẻ gian mạo danh Apple gửi tin nhắn thông báo tìm thấy thiết bị kèm đường link giả mạo để đánh cắp Apple ID.



Cảnh báo chiêu lừa đảo mới khai thác tính năng Find My của Apple.

Theo Trung tâm An ninh mạng quốc gia Thụy Sĩ, những kẻ tấn công đang khai thác lỗ hổng cơ chế của tính năng "Tìm thiết bị" (Find My) của Apple để nhắm mục tiêu vào những người dùng đã báo cáo thiết bị của họ ở trạng thái "Mất" (Lost Mode) hoặc bị đánh cắp.

Khi người dùng kích hoạt chế độ Mất (Lost Mode) trên iPhone, hệ thống cho phép hiển thị thông điệp tùy chỉnh kèm thông tin liên lạc trên màn hình khóa để hỗ trợ quá trình khôi phục. Những kẻ lừa đảo đã lợi dụng chính tính năng này để thực hiện hành vi tấn công lừa đảo (phishing).

Cụ thể, những kẻ lừa đảo sẽ gửi tin nhắn qua dịch vụ iMessage hoặc SMS, mạo danh là đội ngũ hỗ trợ của "Find My". Các tin nhắn này thường chứa các thông số kỹ thuật chính xác của thiết bị bị mất như model, màu sắc hoặc dung lượng bộ nhớ - những thông tin có thể đã được thu thập từ thông báo tùy chỉnh trên màn hình khóa. Tin nhắn thông báo rằng thiết bị đã được "định vị" (located) và bao gồm một đường liên kết (link) để xem vị trí của thiết bị. Khi nạn nhân nhấp vào URL này, họ sẽ bị chuyển hướng đến một trang web giả mạo được thiết kế để thu thập thông tin đăng nhập của Apple ID và mật khẩu, từ đó giành được quyền truy cập vào tài khoản của người dùng.

Các chuyên gia khuyến nghị người dùng cần xác minh tính xác thực của mọi thông báo khôi phục thiết bị. Tuyệt đối không nhập thông tin Apple ID trên các trang web được truy cập qua đường liên kết trong tin nhắn SMS/iMessage không xác định. Luôn truy cập ứng dụng "Find My" hoặc trang web iCloud chính thức để kiểm tra trạng thái thiết bị bị mất./.

MỘT SỐ LƯU Ý KHI SỬ DỤNG WIFI CÔNG CỘNG

Hiện nay, các cửa hàng cà phê, khách sạn, trung tâm mua sắm, sân bay và nhiều địa điểm khác thường cung cấp cho khách hàng quyền truy cập Wifi công cộng miễn phí. Từ đó, khi sử dụng các dịch vụ tại những nơi này, người dùng vẫn có thể kiểm tra email, truy cập mạng xã hội hoặc lướt web một cách thuận tiện.

Tuy nhiên, tin tặc sẽ thường theo dõi các mạng Wifi công cộng và chặn bắt dữ liệu được truyền qua mạng. Bằng cách này, tin tặc có thể truy cập thông tin tài khoản ngân hàng, mật khẩu và các thông tin có giá trị khác của người dùng.

Để đảm bảo an toàn khi sử dụng Wifi công cộng đội ngũ chuyên gia bảo mật Internet của Kaspersky Lab đưa ra lời khuyên:

Nhận thức được sự nguy hiểm: Wifi công cộng vốn không được an toàn, do đó hãy thận trọng khi sử dụng.



Một số lưu ý khi sử dụng Wifi công cộng.

Bất kỳ thiết bị nào cũng có thể bị tấn công: Tất cả các thiết bị như máy tính xách tay, điện thoại thông minh và máy tính bảng đều có thể gặp rủi ro khi sử dụng Wifi công cộng.

Thận trọng với tất cả các kết nối Wifi: Không nên tin tưởng các kết nối Wifi là hợp pháp. Nó có thể là một kết nối giả mạo đã được thiết lập bởi tin tặc nhằm thu thập thông tin cá nhân có giá trị từ những người dùng thiếu thận trọng. Hãy nghi ngờ và thận trọng với mọi kết nối Wifi và không kết nối với những Wifi chưa được xác định, nhận diện. Không dùng wifi công cộng để chuyển tiền online và các công việc cần sự bảo mật cao.

Tìm hiểu và xác thực kết nối Wifi đó là hợp pháp: Một số kết nối giả mạo đã được thiết lập bởi tin tặc sẽ có tên tương tự như quán cà phê, khách sạn hoặc địa điểm cung cấp Wifi miễn phí. Nếu có thể nói chuyện với nhân viên của địa điểm cung cấp kết nối Wifi công cộng đó, thì người dùng cần hỏi thông tin về điểm truy cập Wifi hợp pháp như tên kết nối và địa chỉ IP.

Sử dụng mạng riêng ảo (VPN): Bằng cách sử dụng VPN khi kết nối với mạng Wifi công cộng, người dùng sẽ sử dụng một luồng mạng (tunnel) riêng tư, mã hóa tất cả dữ liệu đi qua mạng. Điều này có thể giúp ngăn chặn việc chặn bắt và thu thập dữ liệu của người dùng.

Tránh sử dụng một số trang web cụ thể: Người dùng nên tránh đăng nhập vào các trang web mà tin tặc sẽ có khả năng thu thập danh tính, mật khẩu hoặc thông tin cá nhân như các trang mạng xã hội, dịch vụ ngân hàng trực tuyến hoặc các trang web lưu trữ thông tin thẻ tín dụng.

Cân nhắc sử dụng dữ liệu di động: Trong trường hợp bắt buộc cần truy cập vào các trang web có lưu trữ hoặc yêu cầu nhập thông tin nhạy cảm, người dùng nên sử dụng dữ liệu di động thay vì kết nối Wifi công cộng.

Bảo vệ thiết bị khỏi các cuộc tấn công mạng: Đảm bảo tất cả các thiết bị được bảo vệ bởi các giải pháp đảm bảo an toàn và chống phần mềm độc hại có hiệu quả, cũng như cần cập nhật chúng thường xuyên nhất có thể.

Nhóm chuyên gia bảo mật của Kaspersky Lab

DỰ BÁO CÁC MỐI ĐE DỌA VÀ THÁCH THỨC AN NINH MẠNG NĂM 2025

Google Cloud đã công bố Dự báo An ninh mạng năm 2025, cung cấp phân tích chi tiết về bối cảnh mối đe dọa mới nổi và các xu hướng bảo mật chính mà các tổ chức trên toàn thế giới nên chuẩn bị, trong đó trí tuệ nhân tạo (AI), địa chính trị và tội phạm mạng là những yếu tố trọng tâm. Báo cáo cũng đã thông tin chi tiết về chiến thuật của tội phạm mạng, đưa ra khuyến nghị giúp tăng cường bảo mật trong năm tới.

Gia tăng các cuộc tấn công mạng do AI điều khiển

Báo cáo nhấn mạnh sự thay đổi trong bối cảnh an ninh mạng, sự trỗi dậy của AI giống như một con dao hai lưỡi. Trong khi AI cung cấp các công cụ mới cho những người bảo vệ, thì nó cũng cung cấp cho tin tặc các khả năng tiên tiến hơn để phát triển các cuộc tấn công.

Phil Venables, Phó Chủ tịch TI Security & CISO, Google Cloud, nhận định rằng: “Năm 2025 sẽ là năm mà AI chuyển từ giai đoạn thí điểm và nguyên mẫu sang áp dụng trên diện rộng”. Điều này sẽ mở ra kỷ nguyên mới của các hoạt động bảo mật bán tự động. Sự tích hợp AI này sẽ giúp tự động hóa các tác vụ, phân tích các tập dữ liệu lớn và hợp lý hóa quy trình làm việc, cuối cùng cho phép các nhóm bảo mật làm việc hiệu quả hơn.

Tuy nhiên, báo cáo cũng cảnh báo về sự gia tăng các cuộc tấn công mạng sử dụng AI. Những kẻ tấn công có thể tận dụng AI, bao gồm các mô hình ngôn ngữ lớn (LLM) và deepfake để tăng cường các cuộc tấn công kỹ nghệ xã hội, tiến hành nghiên cứu lỗ hổng và phát triển phần mềm độc hại tinh vi hơn. Tin tặc cũng sẽ tận dụng deepfake để đánh cắp danh tính, gian lận và vượt qua các biện pháp bảo mật.

Sunil Potti, Phó Chủ tịch, Tổng Giám đốc bộ phận Bảo mật đám mây của Google cho biết: “Năm 2025 là năm đầu tiên chúng ta thực sự chứng kiến giai đoạn thứ hai của AI hoạt động trong lĩnh vực bảo mật”.



Xung đột địa chính trị thúc đẩy các cuộc tấn công mạng phức tạp.

Năm 2025, dự báo căng thẳng địa chính trị sẽ tiếp tục ảnh hưởng sang không gian mạng, thúc đẩy sự phức tạp trong bối cảnh các mối đe dọa an ninh mạng hiện nay. Báo cáo dự đoán hoạt động mạng liên tục từ bốn quốc gia có tiềm lực không gian mạng lớn bao gồm: Nga, Trung Quốc, Iran và Triều Tiên sẽ làm gia tăng các mối đe dọa an ninh mạng khi họ theo đuổi các mục tiêu địa chính trị của mình.

Các tác nhân ủng hộ Trung Quốc dự kiến sẽ tiếp tục sử dụng các chiến thuật bao gồm việc sử dụng các lỗ hổng zero-day và phần mềm độc hại tùy chỉnh được thiết kế cho các hệ thống nhúng. Các chiến dịch thông tin dự kiến sẽ nhắm mục tiêu trực tiếp đến các cuộc bầu cử và cử tri ở các quốc gia, khu vực được coi là ưu tiên chiến lược hàng đầu của Trung Quốc, đặc biệt là Đài Loan và Mỹ.

Năm 2025, xung đột tại Ukraine có khả năng sẽ tiếp tục là trọng tâm chính trong các nỗ lực gián điệp mạng, tấn công mạng và hoạt động thông tin của Nga. Ngoài Ukraine, các hoạt động gián điệp mạng của Nga gần như chắc chắn sẽ tiếp tục phục vụ lợi ích toàn cầu của Moscow, nhắm đến các chính phủ, chính trị gia, xã hội dân sự, nhà báo, các cơ quan truyền thông và các tổ chức công nghệ, chủ yếu ở châu Âu và các quốc gia thành viên NATO.

Iran sẽ tiếp tục hoạt động mạng liên quan đến cuộc xung đột Israel-Hamas trong khi cũng tập trung vào các tổ chức chính phủ và viễn thông ở Trung Đông và Bắc Phi. Các tác nhân mạng của Triều Tiên sẽ tiếp tục đặt trọng tâm lớn vào việc tấn công chuỗi cung ứng, thường sử dụng các gói phần mềm mã nguồn mở bị cài mã độc trong các chiến dịch tấn công kỹ nghệ xã hội nhắm vào các nhà phát triển phần mềm. Ngoài ra, tin tặc Triều Tiên sẽ tiếp tục tìm kiếm nguồn thu nhập thông qua các hoạt động xâm nhập mạng và đánh cắp tiền điện tử.

Gia tăng các hoạt động tấn công ransomware và đánh cắp thông tin người dùng:

Tội phạm mạng vẫn là mối đe dọa đáng kể, trong đó ransomware và tổng tiền được dự đoán sẽ trở thành những tác nhân gây gián đoạn lớn vào năm 2025. Báo cáo nhấn mạnh sự mở rộng phạm vi ảnh hưởng của các mối đe dọa này, do sự xuất hiện của các dịch vụ ransomware mới và sự gia tăng các trang web lừa đảo.

Báo cáo cũng đưa ra cảnh báo về mối đe dọa ngày càng tăng của phần mềm độc hại đánh cắp thông tin của người dùng. Các chương trình tinh vi này được thiết kế để đánh cắp thông tin nhạy cảm như: thông tin đăng nhập, thông tin cá nhân, tài khoản ngân hàng... gây ra rủi ro đặc biệt cho các cá nhân, tổ chức không có xác thực đa yếu tố mạnh mẽ.

Mã độc đánh cắp thông tin ngày càng tinh vi hơn với các kỹ thuật chống phát hiện và khả năng vượt qua các hệ thống phát hiện điểm cuối. Tội phạm mạng đang nhanh chóng áp dụng các công nghệ tiên tiến, bao gồm AI, mô hình phần mềm độc hại dưới dạng dịch vụ và các kỹ thuật rửa tiền tinh vi, đặt ra thách thức ngày càng tăng đối với các chuyên gia thực thi pháp luật và an ninh.

Một số khuyến nghị giúp bảo đảm an ninh mạng cho năm 2025

Dự báo an ninh mạng của Google Cloud năm 2025 kêu gọi các tổ chức hành động để tăng cường phòng thủ và chủ động giải quyết các mối đe dọa mới nổi với các khuyến nghị như sau:

Ưu tiên bảo mật đám mây: Các tổ chức cần ưu tiên triển khai các nền tảng bảo mật như Hệ thống quản lý thông tin và sự kiện bảo mật và Hệ thống tự động hóa, điều phối và phản hồi an ninh. Những giải pháp này không chỉ giúp cải thiện khả năng hiển thị hệ thống mà còn tăng cường khả năng phát hiện mối đe dọa và xử lý nhanh chóng khi có sự cố xảy ra. Việc tích hợp bảo mật gốc trong hạ tầng đám mây là bước đi chiến lược nhằm đối phó với những mối nguy tiềm ẩn trong môi trường số ngày nay.

Tăng cường quản lý danh tính và quyền truy cập: Triển khai xác thực đa yếu tố là một trong những biện pháp mạnh mẽ để giảm nguy cơ xâm nhập trái phép. Việc yêu cầu thêm một hoặc nhiều yếu tố xác minh (chẳng hạn như mã OTP, sinh trắc học hoặc thiết bị xác thực) giúp tăng cường thêm một lớp bảo mật đáng tin cậy. Bên cạnh đó, các tổ chức cần thường xuyên kiểm tra và đánh giá mức độ rủi ro liên quan đến quản lý danh tính và quyền truy cập. Điều này bao gồm việc xác định những tài khoản hoặc quyền truy cập có nguy cơ cao bị khai thác, đảm bảo rằng chỉ những người thực sự cần thiết mới được quyền truy cập vào tài sản quan trọng. Kiểm soát quyền truy cập chặt chẽ: Áp dụng nguyên tắc "ít quyền nhất" (Least Privilege), đảm bảo mỗi người dùng chỉ có quyền truy cập đúng với nhiệm vụ của họ. Thực hiện giám sát quyền truy cập liên tục, kịp thời thu hồi quyền truy cập không cần thiết

hoặc của những tài khoản không còn hoạt động. Tích hợp giải pháp quản lý truy cập theo vai trò hoặc nhận diện theo ngữ cảnh (Context-Aware Access) để đảm bảo quyền truy cập phù hợp và an toàn.

Chuẩn bị cho mật mã hậu lượng tử: Các ứng dụng điện toán lượng tử trở nên đầy hứa hẹn trên nhiều lĩnh vực khác nhau, từ mật mã và các vấn đề tối ưu hóa đến trí tuệ nhân tạo...Cuộc đua khai thác sức mạnh của điện toán lượng tử đã tạo nên làn sóng đổi mới và hợp tác, tập hợp các chuyên gia về vật lý, khoa học máy tính và kỹ thuật để khai thác toàn bộ tiềm năng của công nghệ đột phá này. Máy tính lượng tử với khả năng thực hiện các phép tính phức tạp ở tốc độ mà máy tính cổ điển không thể đạt được, có khả năng bẻ khóa các phương pháp mã hóa truyền thống được sử dụng rộng rãi, gây ra mối đe dọa đáng kể đến quyền riêng tư và bảo mật thông tin nhạy cảm. Các tổ chức phải bắt đầu đánh giá những rủi ro do điện toán lượng tử gây ra và lập kế hoạch áp dụng các giải pháp mật mã chống lượng tử để bảo vệ dữ liệu nhạy cảm trong thời gian dài.

Luôn cập nhật thông tin và thích ứng: Môi trường an ninh mạng luôn thay đổi, đòi hỏi các tổ chức không ngừng cập nhật thông tin tình báo về mối đe dọa và theo sát các xu hướng rủi ro mới. Các chiến thuật tấn công của tin tặc ngày càng tinh vi, vì vậy việc điều chỉnh chiến lược bảo mật, nâng cấp các biện pháp phòng ngừa và tận dụng thông tin tình báo sẽ giúp tổ chức giữ vững khả năng bảo vệ trước mọi thách thức mới.

Báo cáo Dự báo an ninh mạng của Google Cloud năm 2025 cung cấp cho các nhà quản lý các kiến thức và hiểu biết cần thiết để ứng phó trong bối cảnh an ninh mạng phức tạp. Đồng thời chủ động giải quyết các mối đe dọa mới nổi. Bằng cách áp dụng phương pháp tiếp cận chủ động và toàn diện đối với an ninh mạng, các tổ chức, doanh nghiệp có thể giảm thiểu rủi ro, nâng cao khả năng phục hồi và bảo vệ tài sản có giá trị của mình trong năm 2025./.

TS. Nguyễn Tiến Dũng (Học Viện Cảnh sát nhân dân)

CÔNG ƯỚC HÀ NỘI:

DẤU MỐC LỊCH SỬ KIẾN TẠO TRẬT TỰ PHÁP LÝ TOÀN CẦU VỀ AN NINH MẠNG

Lần đầu tiên trong lịch sử, Liên hợp quốc chọn Hà Nội làm nơi mở ký một công ước toàn cầu. Công ước Hà Nội về chống tội phạm mạng không chỉ khẳng định vị thế và trách nhiệm của Việt Nam, mà còn mở ra kỷ nguyên hợp tác mới cho an ninh và công lý trong thế giới số.



Chủ tịch nước Lương Cường, Tổng thư ký Liên hợp quốc và lãnh đạo, đại diện các nước tham dự Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng.

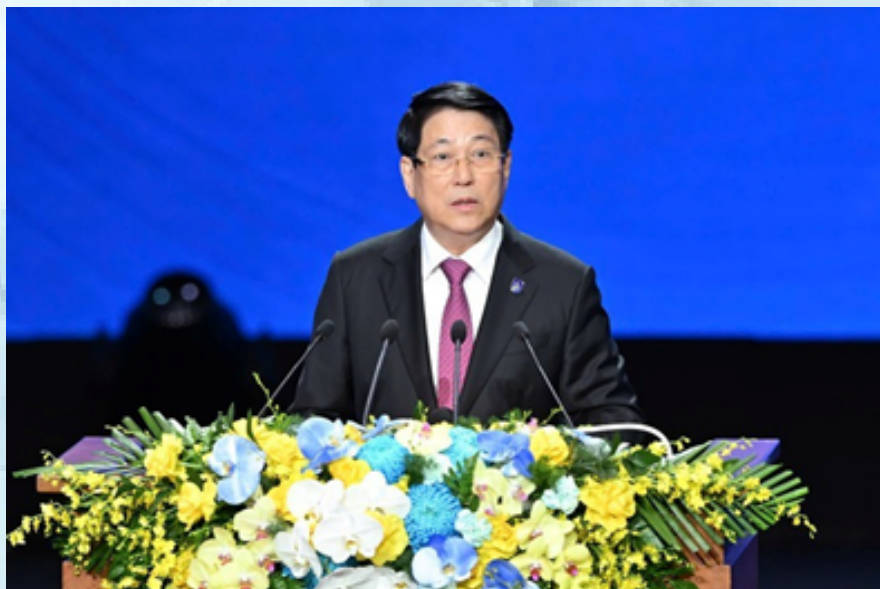
(Ảnh: Thuỷ Nguyễn)

Từ Hà Nội, thành phố của hòa bình, thế giới đã chứng kiến một cột mốc mang tầm lịch sử. Lễ ký kết Công ước Liên hợp quốc về chống tội phạm mạng, được tổ chức vào ngày 25-26/10/2025, là một công ước đa phương toàn cầu về tội phạm mạng được ký kết, đánh dấu bước ngoặt lớn trong nỗ lực xây dựng khuôn khổ pháp lý quốc tế nhằm bảo đảm an ninh mạng, công lý và nhân quyền trong kỷ nguyên số.

Công ước Hà Nội ra đời trong bối cảnh thế giới đang chịu sức ép từ sự bùng nổ công nghệ và những mối đe dọa ngày càng tinh vi của tội phạm mạng. Các vụ tấn công dữ liệu, lừa đảo điện tử, tống tiền bằng mã độc hay lợi dụng tiền mã hóa để rửa tiền gây thiệt hại hàng nghìn tỷ USD mỗi năm. Không gian mạng từ chỗ là nền tảng phát triển, đang dần trở thành “mặt trận mới” của các cuộc xung đột phi truyền thống. Chính vì vậy, việc Liên hợp quốc, thông qua và tổ chức ký kết Công ước Hà Nội, không chỉ là bước tiến pháp lý, mà còn là biểu tượng cho tinh thần đoàn kết và hợp tác toàn cầu trong bảo vệ môi trường số an toàn, nhân văn.

Lễ ký kết tại Trung tâm Hội nghị Quốc gia Hà Nội thu hút hơn 110 quốc gia, trong đó có Tổng Thư ký Liên hợp quốc António Guterres và Chủ tịch nước Việt Nam Lương Cường.

Với chủ đề “Chống tội phạm mạng-Chia sẻ trách nhiệm-Bảo đảm tương lai của chúng ta”. Sự kiện ghi dấu Việt Nam là quốc gia đầu tiên ở Đông Nam Á được chọn làm địa điểm đặt tên và mở ký một công ước toàn cầu của Liên hợp quốc, điều chưa từng có tiền lệ. Đến thời điểm kết thúc lễ, 65 quốc gia đã đặt bút ký tham gia, vượt xa con số tối thiểu 40 quốc gia được kỳ vọng để công ước có hiệu lực.



Chủ tịch nước Lương Cường phát biểu tại Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng. (Ảnh: Thuỷ Nguyên).

Tên gọi “Công ước Hà Nội” mang ý nghĩa biểu trưng sâu sắc, không chỉ vinh danh thành phố vì hòa bình mà còn ghi nhận vai trò lãnh đạo, trách nhiệm và bản lĩnh của Việt Nam trong lĩnh vực an ninh mạng toàn cầu. Từ năm 2019, Việt Nam đã tích cực tham gia quá trình đàm phán, đóng góp các đề xuất thiết thực về hỗ trợ kỹ thuật, chuyển giao công nghệ và bảo vệ quyền con người trong không gian mạng. Việc lựa chọn Hà Nội làm nơi mở ký là sự ghi nhận nỗ lực của một quốc gia đang phát triển nhưng luôn kiên định với giá trị hợp tác, pháp quyền và phát triển bền vững.

Công ước Hà Nội gồm 9 chương với 71 điều khoản, quy định toàn diện các vấn đề về hình sự hóa tội phạm mạng, thẩm quyền điều tra, hợp tác quốc tế, dẫn độ, hỗ trợ tư pháp và bảo vệ dữ liệu cá nhân. Văn kiện này không chỉ chuẩn hóa khái niệm tội phạm mạng mà còn thiết lập cơ chế phối hợp xuyên biên giới để các quốc gia có thể chia sẻ thông tin, truy vết và xử lý tội phạm hiệu quả hơn. Các hành vi như truy cập trái phép, đánh cắp dữ liệu, gian lận điện tử, tấn công cơ sở hạ tầng trọng yếu, sử dụng không gian mạng để tuyên truyền khủng bố hay rửa tiền bằng tiền mã hóa đều được định danh cụ thể.

Đây là bước tiến đột phá giúp khắc phục tình trạng “vùng xám pháp lý” từng khiến nhiều vụ tấn công mạng xuyên quốc gia không thể truy tố.

Điểm nổi bật của Công ước Hà Nội là sự cân bằng giữa an ninh và quyền con người. Nếu Công ước Budapest (2001), văn kiện quốc tế đầu tiên về tội phạm mạng, bị phê phán vì thiếu quy định bảo vệ quyền riêng tư và ban đầu chủ yếu dành cho các nước châu Âu thì Công ước Hà Nội đã khắc phục triệt để bằng việc yêu cầu mọi biện pháp điều tra, thu thập dữ liệu phải tuân thủ nguyên tắc pháp quyền, tỉ lệ và minh bạch. Các cơ quan chức năng chỉ được phép tiếp cận dữ liệu cá nhân hoặc giám sát thông tin khi có lệnh tư pháp hợp pháp và trong phạm vi cần thiết. Điều này thể hiện một cách tiếp cận nhân văn, coi an ninh mạng không thể tách rời khỏi quyền con người, đồng thời củng cố niềm tin vào pháp quyền quốc tế.

Từ góc độ pháp lý, Công ước Hà Nội được ví như bộ khung pháp luật toàn cầu đầu tiên về tội phạm mạng, trong đó yêu cầu các quốc gia thành viên phải nội luật hóa các quy định của công ước vào hệ thống pháp luật quốc gia, bảo đảm tính tương thích và đồng bộ. Khi công ước chính thức có hiệu lực, các nước sẽ bước vào giai đoạn triển khai, bao gồm sửa đổi luật hình sự, thiết lập cơ chế dẫn độ và hỗ trợ tư pháp lẫn nhau. Văn phòng Liên hợp quốc về Ma túy và Tội phạm (UNODC) sẽ đóng vai trò trung tâm trong việc giám sát, hỗ trợ kỹ thuật, đào tạo và chuyển giao công nghệ để các quốc gia, đặc biệt là những nước đang phát triển, có đủ năng lực thực thi.

Đối với Việt Nam, Công ước Hà Nội mở ra cơ hội lớn để hoàn thiện khung pháp lý về an ninh mạng, bảo vệ dữ liệu cá nhân và nâng cao năng lực ứng phó với tội phạm công nghệ cao. Bộ Công an cùng các cơ quan liên quan đã bắt đầu xây dựng kế hoạch triển khai, thành lập nhóm công tác liên ngành để rà soát, nội luật hóa các điều khoản đồng thời chuẩn bị nguồn lực kỹ thuật và nhân sự cho quá trình thực thi. Thành công trong vai trò quốc gia đăng cai cũng đưa Việt Nam trở thành một trong những trung tâm hợp tác khu vực về an ninh mạng do UNODC điều phối giai đoạn 2026-2030.

Công ước Hà Nội còn thể hiện tầm nhìn của chủ nghĩa đa phương và tinh thần hợp tác bình đẳng giữa các quốc gia. Trong thời điểm thế giới đang chứng kiến sự chia rẽ về tiêu chuẩn công nghệ giữa các cường quốc, việc



Tổng Thư ký Liên hợp quốc Antonio Guterres phát biểu tại Lễ mở ký Công ước của Liên hợp quốc về chống tội phạm mạng. (Ảnh: Thủy Nguyễn.)

hơn 60 quốc gia cùng ngồi lại tại Hà Nội để ký kết một công ước chung là minh chứng mạnh mẽ cho niềm tin vào đối thoại và luật pháp quốc tế.

Từ đây, Hà Nội trở thành biểu tượng của hợp tác số, nơi các quốc gia cùng chia sẻ trách nhiệm bảo vệ tương lai chung trong không gian mạng.

Không chỉ có ý nghĩa pháp lý, Công ước Hà Nội còn mang giá trị nhân văn sâu sắc. Nó xác định rằng công nghệ phải phục vụ con người chứ không được làm tổn hại đến con người. Việc đưa các điều khoản bảo vệ nạn nhân của tội phạm mạng đã mở ra cách tiếp cận toàn diện, lấy con người làm trung tâm. Bằng việc khuyến khích các quốc gia chia sẻ công nghệ, đào tạo nhân lực và tăng cường năng lực cho các nước yếu thế. Công ước Hà Nội đã góp phần thu hẹp khoảng cách, bảo đảm không ai bị bỏ lại phía sau trong kỷ nguyên chuyển đổi số.

Vai trò của Việt Nam trong tiến trình này không chỉ là nước chủ nhà mà còn là người kiến tạo. Việt Nam đã và đang tích cực thúc đẩy đối thoại giữa các nhóm quốc gia, đóng góp ý kiến xây dựng các điều khoản về hỗ trợ kỹ thuật, bảo vệ dữ liệu và cân bằng lợi ích giữa phát triển và an ninh. Với tinh thần “chủ động, tích cực, có trách nhiệm”, Việt Nam một lần nữa khẳng định vị thế là đối tác tin cậy, cầu nối giữa các quốc gia phát triển và đang phát triển trong việc xây dựng trật tự số toàn cầu.

Tổng Thư ký Liên hợp quốc António Guterres từng phát biểu tại lễ ký rằng: “Công ước Hà Nội là minh chứng cho tinh thần hợp tác không biên giới, cho thấy khi các quốc gia cùng hướng về một mục tiêu chung, vì hòa bình và an ninh số, thế giới có thể vượt qua mọi chia rẽ”. Chủ tịch nước Lương Cường khẳng định: “Việt Nam tự hào đóng góp cho nỗ lực toàn cầu nhằm bảo vệ không gian mạng an toàn, vì con người và vì sự phát triển bền vững”.

Nhìn ở tầm dài hạn, Công ước Hà Nội sẽ định hình một trật tự pháp lý mới cho không gian mạng toàn cầu, nơi luật pháp quốc tế trở thành “tấm khiên” bảo vệ hòa bình và công lý trong thế giới số. Từ Hà Nội, thông điệp lan tỏa đi khắp năm châu: An ninh mạng phải gắn liền với quyền con người, và hợp tác quốc tế chính là chìa khóa để bảo đảm tương lai số an toàn, công bằng, nhân văn. Công ước Hà Nội là biểu tượng của niềm tin toàn cầu được khởi nguồn từ Việt Nam, đất nước của hòa bình và trách nhiệm.

Để tổ chức thành công Lễ mở ký và Hội nghị cấp cao Công ước Liên hợp quốc về chống tội phạm mạng (Công ước Hà Nội), không thể không ghi nhận sự đồng hành trách nhiệm và tâm huyết của các doanh nghiệp tài trợ như: VietinBank, PVN, EVN, MB Bank, Agribank, SSI, FPT, VPBank, Gelex, Vietnam Airlines, VIX, BIDV, Viettel và OKX. Sự chung tay của các đơn vị này thể hiện tinh thần hợp tác công-tư trong một sự kiện quốc tế tầm vóc, đồng thời phản ánh vai trò, trách nhiệm xã hội của cộng đồng doanh nghiệp Việt Nam trong việc hiện thực hóa mục tiêu xây dựng không gian mạng an toàn, tin cậy và phát triển bền vững. Nhờ sự đồng hành ấy, Lễ mở ký Công ước Hà Nội trở thành biểu tượng hợp tác toàn cầu kiểu mẫu, góp phần khẳng định uy tín, vị thế và hình ảnh Việt Nam trên trường quốc tế./.

Giang Khôi

AI ĐANG KHUẾCH ĐẠI NGUY CƠ TẤN CÔNG MẠNG THẾ NÀO

Theo các chuyên gia, trí tuệ nhân tạo có thể khiến kẻ tấn công ngày càng dễ dàng tạo mã độc hoặc các công cụ lừa đảo tinh vi, trong khi bên phòng thủ còn loay hoay ứng dụng AI.

Tại hội thảo Lãnh đạo cấp cao Công nghệ thông tin và An toàn thông tin CIO CSO Summit 2025 tuần này, TS Nguyễn Đức Hiên, Phó trưởng Ban Chính sách Chiến lược Trung ương đánh giá sự phát triển của AI đang đặt ra nhiều thách thức, đặc biệt trong lĩnh vực an ninh mạng.

Theo ông, quy mô và tốc độ của các cuộc tấn công sẽ gia tăng khi AI có thể học hỏi, tối ưu hóa chiến thuật và cho phép tin tặc thực hiện các cuộc tấn công tự động. Khi sử dụng dữ liệu để huấn luyện AI, rủi ro vi phạm dữ liệu và quyền riêng tư cũng tăng lên.

“Ngoài ra, có sự gia tăng bất cân đối về năng lực an ninh mạng giữa các quốc gia, khi các nước lớn đầu tư mạnh vào AI phòng thủ”, ông Hiên nói, đồng thời đề cập đến tình trạng chưa có hành lang pháp lý toàn cầu, khu vực về ứng dụng kiểm soát AI trong an ninh mạng, mà chủ yếu đến từ sự phối hợp giữa các quốc gia trong việc xử lý.



Phó trưởng Ban Chính sách Chiến lược Trung ương Nguyễn Đức Hiên phát biểu tại sự kiện. Ảnh: Phi Vân

Ở vai trò đơn vị chuyên môn về an ninh mạng, ông Nguyễn Sơn Hải, Giám đốc Viettel Cyber Security (VCS), nhận định AI còn làm gia tăng sự bất đối xứng giữa bên phòng thủ và những kẻ tấn công.

Theo ông Hải, an ninh mạng luôn là cuộc chơi bất đối xứng, khi người phòng thủ cần bảo vệ một hệ thống rộng lớn, trên toàn bộ các điểm chạm, và phải làm tốt mọi lúc, mọi nơi, trong khi kẻ tấn công chỉ cần một điểm yếu tại một thời điểm là có thể xuyên phá.

Với sự xuất hiện của AI, sự bất đối xứng còn được khuếch đại lên nhiều lần", ông Hải nói, cho rằng công nghệ này đã làm hạ thấp rào cản kỹ thuật, cho phép kẻ tấn công dễ dàng tạo ra công cụ và tiến hành các chiến dịch quy mô lớn với tốc độ tự động hóa cao, trong khi việc sử dụng AI khiến bề mặt tấn công mở rộng nhanh chóng, dữ liệu tập trung, khiến thiệt hại tăng không thể lường trước.

Tại hội thảo, nhiều doanh nghiệp, trong đó có những doanh nghiệp lớn, cũng thừa nhận còn loay hoay trong việc ứng dụng AI vào bảo mật. Trong nửa đầu năm 2025, số liệu từ VCS ghi nhận hơn 8,5 triệu tài khoản tại Việt Nam bị đánh cắp, gần 530.000 cuộc tấn công từ chối dịch vụ và 191 vụ rò rỉ dữ liệu với hơn ba tỷ bản ghi. Con số này gấp gần ba lần cùng kỳ năm 2024. Nhiều hình thức tấn công mới dựa trên AI đã xuất hiện, từ email lừa đảo được cá nhân hóa, deepfake giả mạo, mã độc tự biến đổi, khiến các hệ thống phòng thủ truyền thống gặp nhiều thách thức. Trước đó báo cáo của McKinsey công bố tháng 5/2025 cũng ghi nhận số lượng các vụ tấn công lừa đảo trên toàn cầu đã tăng tới 1.200% kể từ khi AI thể hệ mới xuất hiện vào cuối năm 2022.



Ông Nguyễn Sơn Hải chia sẻ về sự bất đối xứng trong phòng thủ - tấn công mạng trong thời đại AI. Ảnh: Phi Vân

Dùng AI chống lại AI

“Muốn tăng tốc phản ứng, không còn cách nào khác ngoài việc chuyển từ mô hình vận hành thủ công sang vận hành tự động có tích hợp AI”, Giám đốc VCS Nguyễn Sơn Hải nói, nhấn mạnh ứng dụng AI trong vận hành an ninh mạng sẽ là một trong ba trụ cột phòng thủ ở giai đoạn mới, cùng với Zero Trust (Không tin bất kỳ ai) và Cyber Resilience (Khả năng phục hồi mạng).

Trong bối cảnh các nhóm tấn công tích cực sử dụng AI trong hoạt động, việc phòng thủ cũng được khuyến nghị cần ứng dụng mạnh mẽ công nghệ này.

Theo ông Hải, việc ứng dụng AI trong an ninh mạng có trọng tâm nằm ở ba lớp tri thức, gồm: tri thức toàn cầu đến từ các nền tảng AI quốc tế, tri thức bản địa từ kinh nghiệm thực tiễn tại Việt Nam, và dữ liệu ngữ cảnh đặc thù của từng doanh nghiệp. Đây sẽ là bộ ba then chốt giúp AI có thể hỗ trợ đưa ra hành động đúng lúc và phù hợp trong phòng thủ mạng.

Trong khuôn khổ hội thảo, đội ngũ kỹ thuật VCS đã trình diễn hàng loạt nền tảng, là các AI Agent trong phòng thủ thế hệ mới. Trong đó có AI hỗ trợ điều tra, truy vết thông minh, rút ngắn thời gian xử lý cảnh báo từ hàng giờ xuống chỉ 5-10 phút; và AI hỗ trợ kiểm soát tài sản, tự động mở rộng độ phủ giám sát bằng cách tương tác trực tiếp với hệ thống quản trị tập trung. Đây được đánh giá là bước tiến quan trọng hướng tới mô hình SOC thông minh, tự động, hợp nhất, tối ưu nguồn lực con người trong bối cảnh nhân lực an toàn thông tin còn thiếu tại Việt Nam.

Để củng cố nền tảng dữ liệu và tri thức, họ cũng đồng thời ra mắt nền tảng Intel Hub, nơi các tổ chức có thể chia sẻ thông tin tấn công, phối hợp ứng cứu và học hỏi kinh nghiệm từ cộng đồng. Nền tảng đang kết nối hơn 100 tổ chức trong và ngoài nước, từ khối ngân hàng, tài chính, năng lượng, đến các doanh nghiệp công



Giao diện một công cụ sử dụng AI để quản lý các “tài sản” dữ liệu trong doanh nghiệp.

nghe và cơ quan quản lý, cho phép các chuyên gia có thể truy cập dữ liệu về hàng trăm nghìn mẫu mã độc, hàng triệu cảnh báo được cập nhật mỗi ngày, cũng như các dashboard tổng hợp xu hướng tấn công theo từng ngành nghề.

“Ứng dụng AI là tích hợp tri thức an toàn thông tin vào trong ‘cơ thể sống’ của doanh nghiệp”, ông Hải kết luận. “Đây là cách duy nhất để tạo ra lợi thế lâu dài, bền vững hơn so với hacker, những người chỉ dùng AI cho những cuộc tấn công riêng lẻ”/.

Lưu Quý

LỪA ĐẢO MUA SẮM TRỰC TUYẾN TĂNG CAO VÀO DỊP CUỐI NĂM

Tội phạm mạng lợi dụng mùa mua sắm cao điểm để phát tán trang web lừa đảo, nhằm thu thập thông tin cá nhân và dữ liệu thanh toán của người dùng.



Kaspersky phát hiện 6,4 triệu cuộc lừa đảo mua sắm trực tuyến và hơn 20 triệu cuộc tấn công nhắm vào lĩnh vực game trong năm 2025. Ảnh: Nielsen Đồ

Lừa đảo trực tuyến tăng cao ở mùa mua sắm cao điểm cuối năm.

Dữ liệu từ Kaspersky Security Network (KSN) công bố ngày 26.11 cho thấy, từ tháng 1 đến tháng 10 năm 2025, Kaspersky đã chặn tổng cộng 6.394.854 lượt tấn công mạo danh cửa hàng trực tuyến, ngân hàng và hệ thống thanh toán. 48,2% trong số này trực tiếp nhắm vào đối tượng người mua sắm trực tuyến.

Cùng giai đoạn, công ty an ninh mạng này cũng ghi nhận hơn 20 triệu nỗ lực tấn công nhắm vào các nền tảng game, trong đó có 18,56 triệu vụ lợi dụng nền tảng Discord.

Các hoạt động lừa đảo liên quan đến Black Friday tiếp tục diễn ra mạnh mẽ và chiếm phần lớn các chiến dịch tấn công. Trong hai tuần đầu tháng 11, Kaspersky phát hiện 146.535 email spam liên quan đến giảm giá cuối năm, trong đó có 2.572 email về chương trình lễ hội mua sắm nhân Ngày độc thân 11.11.

Nhiều chiến dịch tiếp tục tái sử dụng các kịch bản lừa đảo đã xuất hiện từ những năm trước, như giả mạo những nhà bán lẻ nổi tiếng Amazon, Walmart và Alibaba, hứa hẹn ưu đãi “mua sớm” để dụ người dùng truy cập vào các trang giả mạo.

Hoạt động lừa đảo quy mô lớn sử dụng trang giả mạo nhắm vào các nền tảng giải trí cũng diễn ra mạnh mẽ. Trong năm 2025, Kaspersky ghi nhận 801.148 cuộc tấn công mạo danh Netflix và 576.873 vụ liên quan đến Spotify.

Mối đe dọa không chỉ diễn ra trong lĩnh vực thương mại điện tử. Năm 2025, Kaspersky phát hiện 2.054.336 nỗ lực lừa đảo giả mạo các nền tảng game như Steam, PlayStation và Xbox. Làn sóng phần mềm độc hại nguy hại dưới dạng game cũng trở nên mạnh mẽ hơn với 20.188.897 lượt phát tán bị chặn, trong đó riêng số lượt phát tán qua Discord lên tới 18.556.566 vụ, gấp hơn 14 lần so với năm 2024.

Khuyến nghị cách phòng tránh

Olga Altukhova, chuyên gia phân tích nội dung web cao cấp tại Kaspersky nhận định: “Dữ liệu năm nay cho thấy hoạt động của tội phạm mạng đang diễn ra trên toàn bộ hệ sinh thái số. Chúng bám theo hành vi trực tuyến của người dùng ở mọi nơi - từ sàn thương mại điện tử, dịch vụ game, ứng dụng streaming cho đến các công cụ liên lạc, liên tục điều chỉnh



Mùa mua sắm cao điểm cuối năm cũng là giai đoạn tội phạm mạng thực hiện nhiều hành vi lừa đảo. Ảnh: Nhiên Đỗ

chiến thuật để nguy hại và hòa mình vào những môi trường quen thuộc mà người dùng hay sử dụng nhất.

Điều này đòi hỏi người dùng phải thường xuyên cảnh giác, tuân thủ các nguyên tắc an toàn cơ bản, nhất là trong những giai đoạn hoạt động trực tuyến tăng cao”.

Để tận hưởng mùa Black Friday một cách an toàn và trọn vẹn nhất, các chuyên gia an ninh mạng đã đưa ra các khuyến nghị sau:

- Không vội tin tưởng bất kỳ đường link hay tệp đính kèm nào trong email. Luôn kiểm tra người gửi trước khi mở.

- Kiểm tra lại website mua sắm trước khi nhập thông tin cá nhân: Đường dẫn URL có chính xác không? Có lỗi chính tả hoặc lỗi giao diện nào bất thường không?

- Nếu muốn mua hàng từ một thương hiệu lạ, hãy xem đánh giá từ khách hàng khác trước khi quyết định.

- Kể cả khi đã rất cẩn thận, người dùng vẫn có thể không phát hiện ra vấn đề cho tới khi xem sao kê ngân hàng hoặc thẻ tín dụng. Vì vậy, người dùng nên chủ động kiểm soát tài khoản và kiểm tra giao dịch tài chính, thay vì chờ đợi các báo cáo định kỳ gửi đến qua đường bưu điện.

- Hãy đăng nhập vào tài khoản trực tuyến để kiểm tra: nếu thấy giao dịch nào không hợp lệ, cần liên hệ ngay với ngân hàng hoặc đơn vị phát hành thẻ để kịp thời xử lý./.

Nguyễn Đăng

NÂNG CAO KỸ NĂNG BẢO ĐẢM AN NINH, AN TOÀN TRÊN KHÔNG GIAN MẠNG CỦA SINH VIÊN CÁC TRƯỜNG ĐẠI HỌC, CAO ĐẲNG HIỆN NAY

Sáng 22/8/2025, tại Hội trường số 9, tầng 10, nhà A1, Học viện Báo chí và Tuyên truyền tổ chức Hội thảo khoa học sinh viên chủ đề “Nâng cao kỹ năng bảo đảm an ninh, an toàn trên không gian mạng của sinh viên các trường đại học, cao đẳng hiện nay”.



Quang cảnh Hội thảo khoa học sinh viên

Tham dự Hội thảo có: PGS, TS. Lưu Văn Quảng, Thường vụ Đảng ủy, Phó Giám đốc Học viện; TS. Nguyễn Thị Thu Hường, Trưởng ban Quản lý khoa học và Hợp tác quốc tế; TS. Lữ Đăng Nhạc, Phó Giám đốc Trung tâm Tin học và Ngoại ngữ; TS. Nguyễn Thị Hải Yến, Phó trưởng Ban Quản lý khoa học và Hợp tác quốc tế.



Đoàn chủ tịch điều hành Hội thảo khoa học sinh viên.

Phát biểu khai mạc Hội thảo, PGS, TS. Lưu Văn Quảng, Thường vụ Đảng ủy, Phó Giám đốc Học viện nhấn mạnh, cùng với những lợi ích to lớn mà không gian mạng mang lại, chúng ta cũng đang phải đối mặt với hàng loạt thách thức mới, nguy hiểm hơn và phức tạp hơn. Tình trạng xâm phạm quyền riêng tư, đánh cắp dữ liệu, lừa đảo trực tuyến, lan truyền tin giả, thông tin sai lệch, kích động tư tưởng cực đoan, xuyên tạc đường lối, chính sách của Đảng và Nhà nước... đang diễn ra ngày càng phổ biến với mức độ ngày càng tinh vi.

Những mối đe dọa này không chỉ gây tổn hại về mặt vật chất, ảnh hưởng nghiêm trọng đến tinh thần và sự phát triển lành mạnh của thế hệ trẻ, đặc biệt đối tượng là sinh viên - những người thường xuyên, trực tiếp sử dụng và tương tác với không gian mạng mỗi ngày, mà còn là đối tượng dễ bị lôi kéo vào con đường vi phạm pháp luật.



PGS, TS. Lưu Văn Quảng, Thường vụ Đảng ủy, Phó Giám đốc Học viện phát biểu khai mạc Hội thảo.

Chính vì vậy, việc nâng cao kỹ năng bảo đảm an ninh, an toàn trên không gian mạng cho sinh viên không chỉ là yêu cầu khách quan, mà còn là nhiệm vụ cấp thiết nhằm bảo vệ quyền lợi hợp pháp của sinh viên, xây dựng thể hệ công dân số có bản lĩnh, có đạo đức, có trách nhiệm, góp phần trực tiếp vào thực hiện đường lối của Đảng, chính sách của Nhà nước và công cuộc xây dựng, bảo vệ Tổ quốc trong tình hình mới.

Đồng chí tin tưởng rằng, những tham luận và ý kiến thảo luận tại Hội thảo sẽ giúp sinh viên không chỉ trở thành người sử dụng thông minh, an toàn, mà còn là những "người bảo vệ chủ quyền số" đầy trách nhiệm trong môi trường mạng, góp phần thiết thực vào việc từng bước hình thành nên một thể hệ sinh viên có tri thức, bản lĩnh, đạo đức, biết sử dụng công nghệ để lan tỏa những giá trị tích cực, góp phần bảo vệ lợi ích cá nhân, cộng đồng và đất nước.



TS. Nguyễn Thị Thu Hường, Trưởng ban Quản lý khoa học và Hợp tác quốc tế báo cáo đề dẫn Hội thảo.

Báo cáo đề dẫn Hội thảo, TS. Nguyễn Thị Thu Hường, Trưởng ban Quản lý khoa học và Hợp tác quốc tế nhấn mạnh, Hội thảo cần tập trung làm rõ những nội dung trọng tâm như: Những vấn đề lý luận và thực tiễn liên quan đến an ninh, an toàn trên không gian mạng trong bối cảnh hiện nay; Đánh giá khách

quan, toàn diện thực trạng nhận thức, hành vi và kỹ năng sử dụng không gian mạng của sinh viên hiện nay; Đề xuất những định hướng và giải pháp mang tính đồng bộ, khả thi nhằm nâng cao kỹ năng bảo đảm an ninh, an toàn thông tin cho sinh viên.

Tham luận tại Hội thảo, sinh viên Trần Phương Thảo, Khoa Quan hệ quốc tế đã phân tích những tác động đa chiều của mạng xã hội đến sinh viên Việt Nam, chỉ ra những lợi ích lẫn nguy hại tiềm ẩn và đề xuất các giải pháp thiết thực giúp sinh viên sử dụng mạng xã hội một cách tích cực hơn như: tự rèn luyện kỹ năng số và duy trì sự cân bằng giữa đời sống thực và ảo.



Sinh viên Trần Phương Thảo, Khoa Quan hệ quốc tế đọc tham luận tại Hội thảo.



Sinh viên Phạm Thị Minh Trang, Khoa Kinh tế chính trị đọc tham luận tại Hội thảo.

Tham luận tại Hội thảo, sinh viên Nguyễn Thị Cẩm Ly, Khoa Lịch sử Đảng cho biết, sinh viên dễ bị ảnh hưởng bởi tin giả và các quan điểm sai trái do hạn chế về kiến thức lý luận chính trị và tư duy phản biện yếu, có tâm lý tin vào hiệu ứng đám đông. Do đó, việc nâng cao nhận thức chính trị, phát triển tư duy phản biện, trang bị năng lực số và phát huy vai trò của Đoàn - Hội rất cần thiết, giúp sinh viên chủ động đấu tranh với thông tin xấu độc, qua đó, góp phần bảo vệ nền tảng tư tưởng của Đảng trên không gian mạng.

Tham luận tại Hội thảo, sinh viên Phạm Thị Minh Trang, Khoa Kinh tế chính trị chia sẻ, an ninh mạng sẽ giúp sinh viên bảo vệ thông tin cá nhân, tiếp cận tri thức toàn cầu và phát triển tư duy phản biện. Việc xem nhẹ an ninh mạng sẽ dẫn đến nhiều rủi ro như đánh cắp dữ liệu, lừa đảo, bạo lực mạng, nghiện mạng xã hội và giảm hiệu quả học tập.



Sinh viên Nguyễn Thị Cẩm Ly, Khoa Lịch sử Đảng đọc tham luận tại Hội thảo.



*TS. Lữ Đăng Nhạc, Phó Giám đốc Trung tâm Tin học và Ngoại ngữ
phát biểu tổng kết Hội thảo*

Phát biểu tổng kết Hội thảo, TS. Lữ Đăng Nhạc, Phó Giám đốc Trung tâm Tin học và Ngoại ngữ khẳng định, các tham luận, phát biểu và thảo luận không chỉ nhấn mạnh tầm quan trọng đặc biệt của kỹ năng bảo đảm an ninh, an toàn trên không gian mạng của sinh viên các trường đại học, cao đẳng hiện nay, mà còn chỉ ra những yêu cầu cấp thiết trong việc nâng cao kỹ năng của sinh viên về an ninh, an toàn mạng trong bối cảnh chuyển đổi số. Đồng thời, Hội thảo cũng đã gợi mở nhiều vấn đề quan trọng, những góc nhìn mới về cách thức tiếp cận và triển khai vấn đề này./.

Lê Hằng, Minh Anh

RA MẮT “HỆ THỐNG ĐIỀU HÀNH AN NINH MẠNG QUỐC GIA”

Trong khuôn khổ Ngày An ninh mạng (ANM) Việt Nam, Trung tâm An ninh mạng Quốc gia (Cục An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao (A05), Bộ Công an) đã chính thức ra mắt “Hệ thống điều hành An ninh mạng Quốc gia”.

Đây là một giải pháp toàn diện do chính các chuyên gia trong nước nghiên cứu, phát triển và làm chủ hoàn toàn. Hệ thống này là tâm huyết, kết quả của quá trình nghiên cứu, phát triển và thử nghiệm nội bộ kéo dài gần một năm, với mục tiêu thiết lập một nền tảng điều phối, giám sát và ứng phó sự cố mạng toàn diện, tập trung, mang tính “xương sống” cho an ninh mạng quốc gia.

Thượng tá Lê Xuân Thủy, Giám đốc Trung tâm An ninh mạng Quốc gia, Cục A05 cho biết, trong giai đoạn mới của phát triển đất nước hiện nay, các hệ thống thông tin buộc phải liên thông với nhau về dữ liệu để phục vụ kết nối. Đây là xu thế tất yếu trong chuyển đổi số.

"Khi các hệ thống kết nối với nhau sẽ xuất hiện các rủi ro. Hiện nay các tổ chức, đơn vị đang bảo vệ các hệ thống của mình tương đối độc lập, chưa có một tổ chức đứng ra để kết nối chia sẻ các thông tin, dữ liệu. Theo như chúng tôi thống kê, theo dõi các cuộc tấn công vào các cơ sở hạ tầng trọng yếu thường diễn ra theo chiến dịch, không chỉ một tổ chức. Như vậy việc kết nối trao đổi nhằm



Thượng tá Lê Xuân Thủy phát biểu tại lễ ra mắt Hệ thống điều hành An ninh mạng Quốc gia.

tăng cường công tác đảm bảo hỗ trợ lẫn nhau trong các tình huống khẩn cấp là hết sức cần thiết", Thượng tá Lê Xuân Thủy chia sẻ.

Trên cơ sở đó, Trung tâm An ninh mạng Quốc gia đã phát triển Nền tảng điều phối, ứng phó xử lý sự cố an ninh mạng quốc gia. Đây là hệ thống trung tâm kết nối giữa lực lượng ứng phó xử lý sự cố với các cơ quan, công ty chủ quản tại các hệ thống trọng yếu, các cơ quan nhà nước, chính quyền địa phương các doanh nghiệp cũng như các tổ chức cung cấp dịch vụ SOC (Trung tâm điều hành an ninh) trên cả nước. Từ đó, hình thành nên sự điều phối chung thống nhất dưới sự chỉ đạo của lực lượng chuyên trách đảm bảo an ninh mạng của Bộ Công an. Ngoài ra hệ thống này cũng kết nối với các đơn vị về phân tích, cảnh báo.

Hệ thống này cũng tích hợp với các công cụ hỗ trợ xử lý sự cố trong hệ sinh thái của A05 cũng như tích hợp các nền tảng tri thức về dữ liệu tình báo an ninh mạng khác tăng cường khả năng nhận biết và ra quyết định sớm.

Hệ thống được xây dựng và đưa vào vận hành thí điểm theo nhiều giai đoạn. Từ 1-7-2025, hệ thống đã triển khai cho 34 đơn vị Công an cấp tỉnh, thành phố. Giai đoạn triển khai toàn quốc (từ 6-8-2025 đến năm 2026) sẽ tiếp tục kết nối các Bộ, ngành, chủ quản hệ thống thông tin trọng yếu; bước cuối mở rộng đến doanh nghiệp, nhà cung cấp dịch vụ công nghệ thông tin để hình thành "mạng lưới an ninh" đồng bộ, cộng đồng.

Trong tương lai, hệ thống này sẽ được tích hợp các tính năng hỗ trợ phân tích và ra quyết định bằng trí tuệ nhân tạo (AI), giúp dự đoán và ứng phó sớm hơn. Cùng với đó, Hệ thống sẽ tích hợp với các nền tảng khác như kho dữ liệu mã độc và thông tin tình báo đồng thời mở rộng các kênh tiếp nhận sự cố, từ email, ứng dụng di động đến tích hợp API./.

Hồng Quang

CÁC NGUY CƠ MẤT AN TOÀN PHỔ BIẾN MÀ NGƯỜI DÙNG CẦN CẢNH GIÁC KHI THAM GIA MÔI TRƯỜNG MẠNG LÀ GÌ?

Trả lời:

Thứ nhất, lừa đảo trực tuyến: Đây là hành vi lừa gạt người dùng cung cấp thông tin cá nhân, tài chính hoặc nhấp vào liên kết độc hại. Các đối tượng có thể giả mạo email, trang web, tin nhắn rác... để chiếm đoạt thông tin.



Thứ hai, phần mềm độc hại: Là các chương trình được tạo ra nhằm gây hại cho máy tính hoặc đánh cắp dữ liệu cá nhân. Người dùng dễ bị nhiễm phần mềm độc hại khi truy cập các trang web không an toàn, tải phần mềm từ nguồn không rõ ràng hoặc mở tệp đính kèm lạ.

Thứ ba, rò rỉ thông tin cá nhân: Việc để lộ dữ liệu như họ tên, số điện thoại, tài khoản ngân hàng, mật khẩu... có thể khiến người dùng bị lợi dụng để thực hiện hành vi gian lận, trộm cắp danh tính hoặc sử dụng vào mục đích phi pháp.

Thứ tư, nội dung bạo lực, đe dọa, bắt nạt trên mạng: Không gian mạng có thể bị biến thành nơi phát tán các hành vi tiêu cực như chửi bới, bôi nhọ, đe dọa hoặc bắt nạt. Điều này gây ảnh hưởng nghiêm trọng đến tinh thần, đặc biệt đối với thanh thiếu niên.

Thứ năm, thông tin sai sự thật, xấu, độc: Các thông tin chưa được kiểm chứng có thể lan truyền nhanh chóng, gây hoang mang dư luận. Người dùng cần tỉnh táo, xác minh thông tin từ các nguồn chính thống trước khi chia sẻ.

Thứ sáu, nguy cơ nghiện Internet: Việc sử dụng mạng quá mức có thể ảnh hưởng đến sức khỏe thể chất, tinh thần và các mối quan hệ xã hội, làm giảm hiệu quả học tập và công việc./.

CẦN LÀM GÌ ĐỂ TỰ BẢO VỆ MÌNH TRƯỚC CÁC MỐI NGUY HẠI TRÊN KHÔNG GIAN MẠNG?



Đừng quên bật tính năng xác thực hai yếu tố.

Trả lời: Cần chủ động trang bị một số kỹ năng cơ bản sau:

- Sử dụng mật khẩu mạnh: kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt, dài tối thiểu 12 ký tự; không nên dùng thông tin cá nhân như tên hoặc ngày sinh.
- Cài đặt và cập nhật phần mềm diệt virus thường xuyên để bảo vệ thiết bị trước các tệp hoặc đường dẫn độc hại.
- Cần trọng khi chia sẻ thông tin cá nhân, đặc biệt là dữ liệu nhạy cảm như số căn cước công dân, tài khoản ngân hàng, số điện thoại.
- Nâng cao hiểu biết về an toàn thông tin, thường xuyên đọc tài liệu, tham gia các khóa học, chương trình tuyên truyền về an ninh mạng, bảo mật và kỹ năng sử dụng Internet an toàn.

Việc nâng cao nhận thức, kỹ năng và tinh thần cảnh giác khi tham gia môi trường mạng là yếu tố then chốt giúp mỗi người tự bảo vệ bản thân, góp phần xây dựng không gian mạng an toàn, lành mạnh, phục vụ tốt cho đời sống xã hội và sự phát triển chung của đất nước./.

NHỮNG THÓI QUEN TỐT GIÚP DUY TRÌ AN TOÀN TRÊN KHÔNG GIAN MẠNG LÂU DÀI?



An toàn trên không gian mạng đóng vai trò vô cùng quan trọng và cấp thiết.

Trả lời:

Luôn suy nghĩ trước khi đăng tải thông tin lên môi trường mạng.

Một trong những nguyên tắc tối quan trọng để duy trì an toàn trên không gian mạng chính là tư duy cẩn trọng trước khi hành động. Trước khi đăng bất cứ hình ảnh, video, hay chia sẻ suy nghĩ của mình, cần cân nhắc xem nội dung đó có thể gây ảnh hưởng gì đến bản thân hay người khác hay không. Thói quen này giúp hạn chế việc vô tình để lộ thông tin cá nhân, hoặc tạo điều kiện cho kẻ xấu lợi dụng, gây ảnh hưởng tiêu cực.

Thói quen suy nghĩ kỹ càng còn giúp bạn trở thành người dùng mạng có trách nhiệm, biết chọn lọc thông tin, tránh lan truyền các nội dung không phù hợp, ảnh hưởng tiêu cực đến cộng đồng, góp phần nâng cao ý thức cá nhân, xây dựng hình ảnh tích cực trên mạng xã hội, từng bước hình thành một cộng đồng trực tuyến lành mạnh, văn minh, tràn đầy trách nhiệm.

Giữ thái độ tôn trọng, văn minh khi bình luận trên mạng

Trong môi trường mạng, mỗi bình luận, phản hồi đều có thể ảnh hưởng trực tiếp tới cảm xúc, tâm lý của người khác. Do đó, duy trì thái độ tôn trọng, tránh những lời lẽ xúc phạm, công kích, hoặc bình luận mang tính tiêu cực là nguyên tắc vàng trong việc giữ an toàn trên không gian mạng. Sống trong một cộng đồng tràn đầy sự tôn trọng sẽ giúp các thành viên cảm thấy thoải mái, an tâm để chia sẻ và học hỏi lẫn nhau.

Hành xử văn minh không chỉ giúp xây dựng hình ảnh cá nhân tích cực, mà còn góp phần gìn giữ môi trường mạng trong sạch, phù hợp với các tiêu chuẩn đạo đức. Việc này còn giúp giảm thiểu các tranh cãi không cần thiết, hạn chế các hoạt động gây chia rẽ, và xây dựng cộng đồng mạng gắn kết, nhân văn, nơi mọi người đều cảm thấy an toàn và tôn trọng lẫn nhau.

Cập nhật kiến thức bảo mật thường xuyên

Thế giới số luôn thay đổi với tốc độ nhanh chóng, các mối đe dọa về an toàn mạng không ngừng nâng cao, tinh vi hơn qua từng ngày. Vì vậy, việc cập nhật kiến thức, kỹ năng bảo mật là cách tối ưu để duy trì an toàn trên không gian mạng. Cần theo dõi các thông tin mới về các phương thức tấn công, các lỗ hổng bảo mật, và các công nghệ mới để phòng chống hiệu quả.

Điều này còn giúp chủ động thích nghi, đáp ứng tốt các thay đổi của môi trường. Các bạn trẻ, học sinh đặc biệt cần nâng cao ý thức tự học hỏi, tham gia các khóa đào tạo, đọc tài liệu chính thống, hoặc theo dõi các nguồn tin chính đáng để luôn nằm trong tầm kiểm soát về an toàn thông tin cá nhân của mình. Cập nhật kiến thức bảo mật giúp bạn trở thành người dùng thông thái, tự tin và chủ động hơn trong việc bảo vệ chính mình trên không gian mạng.

Trong thế giới số ngày nay, an toàn trên không gian mạng đóng vai trò vô cùng quan trọng và cấp thiết. Bằng việc tuân thủ các nguyên tắc vàng như không chia sẻ thông tin cá nhân quá mức, kiểm tra nguồn tin chính xác, đặt mật khẩu mạnh, cẩn thận khi trò chuyện, giữ thiết bị an toàn, tham gia các hoạt động đúng cách, và báo cáo kịp thời các sự cố, chúng ta sẽ xây dựng được một cộng đồng mạng bền vững, lành mạnh. Mỗi cá nhân chính là người bảo vệ chính mình và cộng đồng khỏi các hiểm họa ẩn chứa trong mạng internet./.

CÁCH XỬ LÝ KHI VÔ TÌNH NHẬP VÀO MỘT LIÊN KẾT ĐỘC HẠI HOẶC NGHI NGỜ ĐỘC HẠI TRÊN KHÔNG GIAN MẠNG?



Cần cẩn thận trước những tin nhắn kèm theo đường link truy cập

Trả lời:

Khi vô tình nhấp vào một liên kết độc hại hoặc nghi ngờ độc hại hãy nhanh chóng thực hiện như sau:

- Ngay lập tức ngắt kết nối máy tính hoặc thiết bị khỏi mạng internet để ngăn chặn sự lây lan của mã độc.
- Tiến hành thay đổi mật khẩu của tài khoản bị ảnh hưởng ngay lập tức. Nếu sử dụng mật khẩu đó cho các tài khoản khác, hãy lập tức thay đổi tất cả.
- Nhanh chóng chạy một chương trình quét chống virus đáng tin cậy trên thiết bị đang dùng.
- Báo cáo sự cố cho bộ phận phụ trách hoặc nhà cung cấp dịch vụ liên quan./.

XÁC THỰC ĐA YẾU TỐ (MFA) CÓ QUAN TRỌNG KHÔNG?

Trả lời:

Xác thực nhiều yếu tố (MFA) là quy trình đăng nhập tài khoản gồm nhiều bước, yêu cầu người dùng nhập thêm thông tin khác ngoài mật khẩu. Ví dụ: cùng với mật khẩu, người dùng có thể được yêu cầu nhập mã OTP gửi qua email, trả lời câu hỏi bí mật hoặc quét vân tay.



MFA là gì?

So với việc chỉ dùng mật khẩu, MFA tạo thêm lớp bảo vệ thứ hai, giúp ngăn chặn truy cập trái phép ngay cả khi mật khẩu đã bị lộ. Đây là lý do MFA được xem là một trong những biện pháp bảo mật quan trọng nhất hiện nay..

Theo nghiên cứu thực nghiệm do Microsoft Research thực hiện, đối với nhóm người dùng doanh nghiệp quy mô lớn, những tài khoản bật MFA hiếm khi bị chiếm quyền điều khiển, cho thấy mức giảm rủi ro truy cập trái phép rất đáng kể so với tài khoản không bật MFA

Các yếu tố xác thực thường được sử dụng trong MFA gồm có:

Yếu tố bạn biết: Mật khẩu, PIN, câu hỏi bảo mật.

Yếu tố bạn có: Điện thoại dùng ứng dụng OTP, token bảo mật, thiết bị xác thực cầm tay.

Yếu tố sinh trắc học: Vân tay, nhận diện khuôn mặt, quét mống mắt.

Nhờ kết hợp nhiều yếu tố độc lập, MFA giúp giảm mạnh nguy cơ bị chiếm đoạt tài khoản khi mật khẩu bị đánh cắp hoặc bị rò rỉ.

MFA đặc biệt quan trọng đối với: Email, tài khoản ngân hàng, ví điện tử, mạng xã hội, tài khoản thanh toán trực tuyến hoặc tài liệu nội bộ.

Trong môi trường tổ chức, MFA là thành phần cốt lõi của chính sách quản lý truy cập và là tuyến phòng vệ quan trọng nhằm bảo vệ dữ liệu.

Nói cách khác, xác thực đa yếu tố MFA là lớp bảo vệ bổ sung quan trọng và cần thiết, giúp chặn đứng phần lớn nỗ lực xâm nhập, ngay cả khi kẻ tấn công đã có mật khẩu. Vì vậy, người dùng nên chủ động bật MFA trên tất cả dịch vụ quan trọng để tăng cường an toàn cho tài khoản của mình./.