CHUYÊN ĐỀ: AN TOÀN THÔNG TIN VÀ PHÒNG, CHỐNG VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG

I. Nhận thức về an toàn thông tin trên không gian mạng

1. Khái niệm an toàn thông tin

Trong những năm gần đây, Đảng và Nhà nước ta đã có nhiều chủ trương, chính sách và các biện pháp đẩy mạnh phát triển ứng dụng công nghệ thông tin (CNTT), gắn liền với công tác bảo đảm an toàn, an ninh thông tin trên không gian mạng. Nghị quyết số 36-NQ/TW ngày 01/7/2014 của Bộ Chính trị về đẩy mạnh ứng dụng, phát triển CNTT, đáp ứng yêu cầu phát triển bền vững và hội nhập quốc tế đã chỉ rõ "phải gắn kết chặt chẽ việc ứng dụng, phát triển CNTT phải đi đôi với bảo đảm an toàn, an ninh và bảo mật hệ thống thông tin và cơ sở dữ liệu quốc gia", đặc biệt cần "phát huy vai trò các lực lượng chuyên trách bảo vệ an toàn, an ninh thông tin và bí mật nhà nước. Thực hiện cơ chế phối hợp chặt chẽ giữa các lực lượng công an, quân đội, ngoại giao, cơ yếu, thông tin và truyền thông" để có các biện pháp về tổ chức và kỹ thuật, sẵn sàng đối phó với các cuộc chiến tranh thông tin, chiến tranh mạng, bảo đảm chủ quyền quốc gia, trật tự an toàn xã hội.

Theo Nghị định 64-2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng CNTT trong hoạt động của cơ quan nhà nước: "*An toàn thông tin là an toàn kỹ thuật cho các hoạt động của các cơ sở hạ tầng thông tin, trong đó bao gồm an toàn phần cứng và phần mềm theo các tiêu chuẩn kỹ thuật do Nhà nước ban hành; duy trì các tính chất bí mật, toàn vẹn, sẵn sàng của thông tin trong lưu trữ, xử lý và truyền dẫn trên mạng*".

Luật An toàn thông tin mạng được ban hành năm 2015 đã thể chế hóa các chủ trương, đường lối, chính sách của Đảng và Nhà nước về an toàn thông tin, đáp ứng yêu cầu phát triển bền vững kinh tế - xã hội, bảo vệ thông tin và hệ thống thông tin, góp phần bảo đảm quốc phòng, an ninh, chủ quyền và lợi ích quốc gia trên không gian mạng. Theo đó: "*An toàn thông tin mạng là sự bảo vệ thông tin, hệ thống thông tin trên mạng tránh bị truy nhập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép nhằm bảo đảm tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin*".

Ngày 12/6/2018, Luật An ninh mạng được Quốc hội khóa XIV thông qua với tỷ lệ 86.86%, gồm 7 chương, 43 điều, quy định những nội dung cơ bản về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; triển khai hoạt động bảo vệ an ninh mạng và quy định trách nhiệm của cơ quan, tổ chức, cá nhân. Sự ra đời của Luật An ninh mạng là bước đột phá trong lịch sử lập pháp của Việt Nam, đảm bảo quyền và nghĩa vụ công dân trên không gian mạng. Theo đó: "*An ninh mạng là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân*". Khác với Luật An toàn thông tin mạng 2015 với mục đích để bảo vệ sự an toàn thông tin trên 03 phương diện: Tính nguyên vẹn của

thông tin, tính bảo mật thông tin và tính khả dụng của thông tin; Luật An ninh mạng 2018 quy định tập trung vào chống lại các thông tin độc hại, xâm phạm đến an ninh quốc gia, trật tự an toàn xã hội, quyền và lợi ích hợp pháp của các cá nhân, tổ chức, cơ quan trên môi trường mạng.

Xét về khái niệm "*Tội phạm sử dụng công nghệ cao*", hiện nay luật pháp của nhiều nước trên thế giới như Australia, Mỹ, Anh đã có định nghĩa liên quan đến tội phạm này như: Tội phạm công nghệ cao (high-tech crime), Tội phạm máy tính (computer crime), Tội phạm liên quan đến máy tính (computer-related crime); tội phạm mạng (cybercrime)... Trong Luật Hình sự của Australia, tội phạm công nghệ cao (high-tech crime) được định nghĩa là "sự xâm nhập máy tính một cách trái phép; sự sửa đổi trái phép dữ liệu bao gồm việc phá hủy dữ liệu; tấn công từ chối dịch vụ (DoS); tấn công từ chối dịch vụ phân tán (DDoS); tạo ra và phân phối phần mềm độc hại". Theo Từ điển luật học Black's Law, tội phạm máy tính (computer crime) được định nghĩa là: "tội phạm đòi hỏi về kiến thức công nghệ máy tính chẳng hạn như phá hoại hoặc ăn cắp dữ liệu máy tính hay sử dụng máy tính để thực hiện một số tội phạm khác".

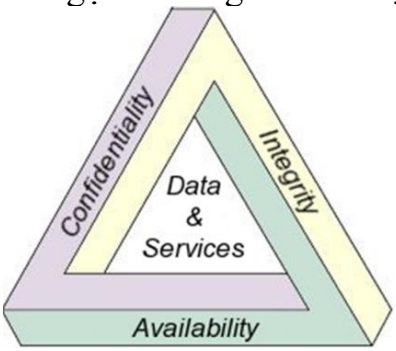
Tại Việt Nam, theo Khoản 1 điều 3 Nghị định số 25/2014/NĐ-CP của Chính phủ ngày 07 tháng 4 năm 2014 quy định: "Tội phạm có sử dụng công nghệ cao là hành vi nguy hiểm cho xã hội được quy định trong Bộ luật Hình sự có sử dụng công nghệ cao". Theo khoản 1 điều 3 của Luật Công nghệ cao năm 2008 quy định: "Công nghệ cao là công nghệ có hàm lượng cao về nghiên cứu khoa học và phát triển công nghệ; được tích hợp từ thành tựu khoa học và công nghệ hiện đại; tạo ra sản phẩm có chất lượng, tính năng vượt trội, giá trị gia tăng cao, thân thiện với môi trường; có vai trò quan trọng đối với việc hình thành ngành sản xuất, dịch vụ mới hoặc hiện đại hóa ngành sản xuất, dịch vụ hiện có".

Theo Từ điển Nghiệp vụ Công an nhân dân Việt Nam (2019), tội phạm sử dụng công nghệ cao là loại tội phạm sử dụng những thành tựu mới của khoa học – kỹ thuật và công nghệ hiện đại làm công cụ, phương tiện để thực hiện hành vi phạm tội một cách cố ý hoặc vô ý, gây nguy hiểm cho xã hội. Chủ thể của loại tội phạm này thường là những người có trình độ học vấn, chuyên môn cao, có thủ đoạn rất tinh vi, khó phát hiện [4].

Giáo trình "Những vấn đề cơ bản về phòng, chống tội phạm sử dụng công nghệ cao" của Học viện Cảnh sát nhân dân (2015) có đề cập đến khái niệm về tội phạm sử dụng công nghệ cao. Theo đó, tội phạm sử dụng công nghệ cao là: "Tội phạm được thực hiện bằng việc cố ý sử dụng tri thức, kỹ năng, công cụ, phương tiện công nghệ thông tin ở trình độ cao tác động trái pháp luật đến thông tin số được lưu trữ, xử lý, truyền tải trong hệ thống máy tính, xâm phạm đến trật tự an toàn thông tin, gây tổn hại lợi ích của Nhà nước, quyền và các lợi ích hợp pháp của các tổ chức, cá nhân" [5].

Nghiên cứu các định nghĩa và khái niệm trên có thể thấy điểm chung trong nội hàm của các khái niệm này đều chỉ các hành vi liên quan đến việc sử dụng máy tính, thiết bị số, khai thác mạng máy tính, mạng viễn thông để gây tổn hại cho lợi ích của các tổ chức, cá nhân và toàn xã hội. Tội phạm sử dụng công nghệ cao là tội phạm sử dụng tri thức, kỹ năng, công cụ, phương tiện công nghệ ở

trình độ cao tác động trái pháp luật đến thông tin, dữ liệu, tín hiệu được lưu trữ, xử lý, truyền tải trong hệ thống mạng máy tính, mạng viễn thông, thiết bị số, xâm phạm đến trật tự an toàn thông tin, gây tổn hại lợi ích của Nhà nước, quyền và các lợi ích hợp pháp của các tổ chức, cá nhân. Trong những hành vi phạm tội sử dụng công nghệ cao có những hành vi tác động trực tiếp đến ba đặc điểm quan trọng nhất của an toàn thông tin (ATTT). ATTT yêu cầu đảm bảo ba đặc điểm là: Tính bí mật (*Confidentiality*), tính toàn vẹn (*Integrity*) và tính sẵn sàng (*Availability*) - được mô hình hóa gọi là tam giác bảo mật CIA.



Hình 1. Tam giác bảo mật CIA

Một giải pháp an toàn bảo mật xây dựng cần nhằm đạt được cả ba mục tiêu cơ bản trên. Cần phân biệt sự khác biệt giữa tính bí mật và tính toàn vẹn. Có những tấn công phá vỡ tính toàn vẹn nhưng không phá vỡ tính bí mật và ngược lại. Nếu ta gửi thông tin trên đường truyền mạng công cộng mà có kẻ bên ngoài xem được thông tin, đó là tính bí mật đã bị vi phạm. Nếu kẻ gian can thiệp sửa đổi, dù chỉ một bit trên những gói tin này và người nhận tin không phát hiện ra sự thay đổi đó, thì tính toàn vẹn đã bị xâm phạm. Mặc dù ta không thể ngăn chặn việc sửa đổi khi các gói tin đi qua các điểm trung gian không thuộc quyền kiểm soát, nếu ta phát hiện được sự thay đổi trái phép, thì ta có thể yêu cầu phát lại. Như vậy tính toàn vẹn vẫn được coi là đảm bảo. Các kỹ thuật mật mã là các công cụ cơ bản nhằm xây dựng dịch vụ đảm bảo tính bí mật và tính toàn vẹn.

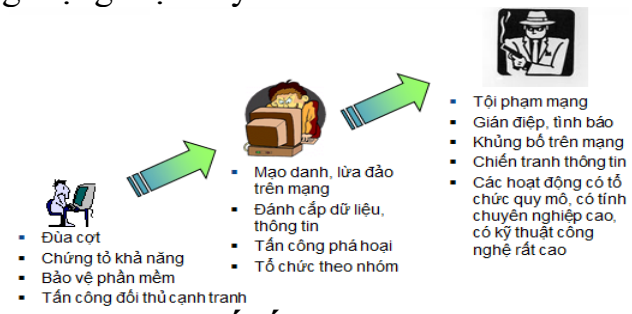
2. Thực trạng an toàn thông tin trong khu vực và trên thế giới

Trong cuộc cách mạng công nghiệp 4.0, thông tin là một dạng tài nguyên. Chính vì thế, đảm bảo an ninh, ATTT là nhiệm vụ quan trọng và cấp thiết. Tuy nhiên hiện nay, các mối đe dọa từ không gian mạng không ngừng tăng lên và thay đổi nhanh chóng. An ninh mạng đang trở thành vấn đề nóng, đặt ra nhiều thách thức đối với tất cả các quốc gia trên toàn thế giới. Tình hình ATTT mạng diễn biến phức tạp, liên tục xảy ra các vụ tấn công, xâm nhập, đánh cắp dữ liệu trên hệ thống mạng của các cơ quan chính phủ, các cơ sở an ninh quốc phòng, tập đoàn kinh tế, cơ quan truyền thông của nhiều quốc gia, như các vụ tấn công vào hệ thống thư điện tử của Bộ Ngoại giao Mỹ, hệ thống máy tính của Nhà trắng, Hạ viện Đức, Bộ Ngoại giao, Bộ Thương mại và Cảnh sát liên bang Australia,…

Các mục tiêu tấn công đã thay đổi, kỹ thuật trở nên phức tạp hơn, hướng tấn công đa dạng hơn và công cụ tấn công được thiết kế chuẩn xác hơn. Những kẻ tấn công đã nghiên cứu kỹ các nạn nhân để có những chiến lược tấn công phù hợp, nhằm tạo ra những ảnh hưởng lớn nhất có thể.

Tài chính là mục tiêu lớn nhất thúc đẩy tin tặc hành động, với 73% số lượng các cuộc tấn công mạng; chính trị, tình báo là mục tiêu lớn thứ hai, với 21% các cuộc tấn công.

Các nhóm tội phạm mạng có tổ chức xuất hiện nhiều hơn. Chiến tranh mạng và đội quân tác chiến mạng cũng được chú trọng hơn. Trong cuộc chạy đua vũ trang trên không gian mạng toàn cầu, các quốc gia đang xây dựng các trung tâm chỉ huy không gian mạng, nhằm củng cố hệ thống phòng thủ chống lại các cuộc tấn công mạng vào các cơ quan và cơ sở hạ tầng. Bên cạnh đó, sự phát triển và phổ biến của mạng xã hội đã làm nảy sinh một nguy cơ ATTT nữa đó là việc lan truyền tin tức giả mạo thông qua mạng xã hội, gây ảnh hưởng đến cá nhân, tổ chức, thậm chí là tình hình an ninh, chính trị của cả một đất nước. Tiền ảo và các hành vi tội phạm liên quan đến tiền ảo cũng đang tiếp tục phát triển, bao gồm lây nhiễm phần mềm độc hại đào tiền ảo tới máy tính, máy chủ; lây nhiễm mã độc đào tiền ảo tới một trang web, sử dụng tài nguyên thiết bị của người tải trang web; đánh cắp tiền từ giao dịch tiền ảo. Hình dưới đây mô tả xu thế chung của tấn công mạng hiện nay.



Hình 2. Xu thế tấn công mạng hiện nay

3. Thực trạng an toàn thông tin ở Việt Nam

Tại Việt Nam, tình hình an toàn an ninh mạng tiếp tục diễn biến phức tạp, tồn tại nhiều cơ sở gây nguy cơ bị tấn công, phá hoại hạ tầng mạng thông tin, ảnh hưởng tới an ninh quốc gia. Báo cáo của hãng bảo mật Kaspersky và Symantec cho thấy, Việt Nam đứng thứ 3 (3,96%) sau Nga (4%) và Ấn Độ (8%) về số người dùng di động bị mã độc tấn công nhiều nhất trên thế giới; thứ 6 trên thế giới về số lượng địa chỉ IP trong nước được dùng trong các mạng máy tính ma tấn công nước khác; thứ 7 trên thế giới về phát tán tin nhắn rác và đứng thứ 12 trên thế giới về các hoạt động tấn công mạng. Đáng chú ý là hoạt động tấn công mạng nhằm vào Việt Nam gia tăng về số lượng, gây nguy cơ bị kiểm soát, khống chế hệ thống thông tin. Tin tặc nước ngoài thường xuyên lợi dụng các điểm yếu về an ninh mạng của hệ thống thông tin điện tử, trang thông tin điện tử của Việt Nam để tấn công, xâm nhập, chiếm quyền điều khiển, chỉnh sửa nội dung.

Năm 2011 có trên 1.500 cổng thông tin Việt Nam bị tin tặc sử dụng mã độc gián điệp dưới hình thức tập tin hình ảnh xâm nhập, kiểm soát, cài mã độc thay đổi giao diện trang chủ. Trong năm 2012 - 2013, Bộ Công an đã phát hiện gần 6.000 lượt cổng thông tin, trang tin điện tử của Việt Nam (trong đó có hơn 300 trang của cơ quan nhà nước) bị tấn công, chỉnh sửa nội dung và cài mã độc. Năm 2014, Bộ Công an phát hiện gần 6.000 trang bị tấn công, chiếm quyền

quản trị, chỉnh sửa nội dung (có 246 trang tên miền gov.vn). Đặc biệt, sau sự kiện giàn khoan HD 981 hạ đặt trái phép trong vùng đặc quyền kinh tế Việt Nam, tin tặc nước ngoài đã tấn công hơn 700 trang mạng Việt Nam và hơn 400 trang trong dịp Quốc khánh (2/9) để chèn các nội dung xuyên tạc chủ quyền của Việt Nam với quần đảo Hoàng Sa. Vào cuối năm 2014, tin tặc cũng đã mở đợt tấn công vào trung tâm dữ liệu của VCCorp khiến nhiều tờ báo mà công ty này đang vận hành kỹ thuật như Dân trí, Người lao động, Soha, VNEconomy, Kenh14… bị tê liệt. Năm 2015 có trên 2.460 website của các cơ quan, doanh nghiệp bị xâm nhập. Nguy cơ từ mã độc và Internet of Things (IoT) bùng nổ tạo "thị trường" lớn cho hacker là hai trong số những nguy cơ an ninh mạng mà người dùng phải đối mặt. Cuối năm 2016, thông tin hơn 73.000 camera IP, trong đó có gần 1.000 camera tại Việt Nam có thể bị theo dõi được công bố rộng rãi. Nguyên nhân là do người dùng chưa có thói quen quan tâm đến an ninh của những thiết bị này, không thay đổi mật khẩu mặc định của hệ thống trước khi kết nối Internet. Bảo mật các thiết bị IoT là rất quan trọng, đặc biệt khi người dùng chưa có thói quen quan tâm đến an ninh cho các thiết bị này.

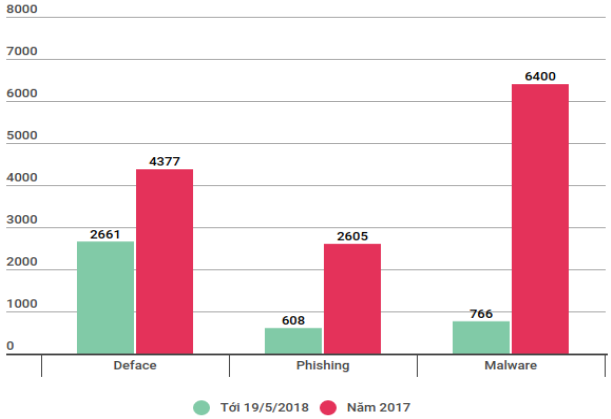
Hình 3. Màn hình thông tin thông báo chuyến bay bị thay đổi giao diện

Trong năm 2016, nổi bật là cuộc tấn công mạng vào một số màn hình hiển thị thông tin chuyến bay tại khu vực làm thủ tục chuyến bay của các sân bay quốc tế Tân Sơn Nhất, Sân bay quốc tế Nội Bài, sân bay quốc tế Đà Nẵng, sân bay Phú Quốc. Các màn hình của sân bay đã bị chèn những hình ảnh và nội dung xuyên tạc về biển Đông. Hệ thống phát thanh của sân bay cũng phát đi những thông điệp tương tự. Đồng thời website của Vietnam Airlines cũng bị tấn công với 411.000 dữ liệu của hành khách đi máy bay đã bị hacker thu thập và phát tán.

Năm 2017 mã độc tống tiền (ransomware) có tên là Wanna Cry trở thành mối nguy hiểm của ngành công nghệ thông tin và nó lây nhiễm với tốc độ chóng mặt ở gần 100 quốc gia, hơn 100 nghìn máy tính. Tại Việt Nam, ghi nhận hơn 100 máy tính bị nhiễm độc. Wanna Cry là một loại mã nhiễm độc tấn công vào máy nạn nhận qua tệp tin đính kèm email hoặc đường link độc hại, như các dòng ransomware khác. Mối nguy hiểm nhất ở mã độc này là nó có khả năng lây nhiễm trên các máy tính ngang hàng. Cụ thể, Wanna Cry sẽ quét toàn bộ các máy tính trong cùng mạng để tìm kiếm thiết bị chứa lỗ hổng của dịch vụ đọc và ghi file từ máy trạm yêu cầu đến máy chủ trong hệ thống Windows. Từ đó, mã độc có thể lây lan vào các máy có lỗ hổng mà không cần người dùng phải thao tác trực tiếp với file đính kèm hay link độc hại.

Hình 4. Màn hình thông tin đòi tiền chuộc khi nhiễm mã độc WannaCry

Năm 2018, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên mức kỷ lục 14.900 tỷ đồng, tương đương 642 triệu USD, nhiều hơn 21% so với mức thiệt hại của năm 2017. Đây là kết quả được đưa ra từ chương trình đánh giá an ninh mạng do Tập đoàn công nghệ Bkav thực hiện tháng 12/2018. Trên phạm vi toàn cầu, tội phạm mạng gây thiệt hại lên tới khoảng 600 tỷ USD mỗi năm, tương đương 0,8% GDP toàn cầu. Trong đó, khu vực Đông Á thiệt hại ước tính từ 120 – 200 tỷ USD, tương đương 0,53 – 0,89% GDP khu vực. Mức thiệt hại 642 triệu USD tương đương 0,26% GDP của Việt Nam tuy chưa phải cao so với khu vực và thế giới, nhưng cũng là kỷ lục đáng báo động. 60% hệ thống mạng cơ quan, doanh nghiệp bị nhiễm mã độc đào tiền ảo. Theo Bkav, có tới hơn 60% cơ quan, doanh nghiệp tại Việt Nam bị nhiễm mã độc đào tiền ảo. Trung bình cứ 10 cơ quan, doanh nghiệp, thì có 6 nơi bị mã độc chiếm quyền điều khiển máy tính đào tiền ảo, gây mất an ninh thông tin.



Hình 5. Tình hình an toàn thông tin tại Việt Nam năm 2017 – 2018

Trong năm 2019, số cuộc tấn công mạng vào các hệ thống thông tin Việt Nam có chiều hướng giảm. Trong 6 tháng đầu năm 2019, Bộ TT&TT ghi nhận 3.159 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam, giảm 2.684 cuộc, tương đương 45,9% so với cùng kỳ năm 2018. Theo Cục ATTT (Bộ TT&TT) trong 4 tháng đầu năm 2020 tổng cộng 1.056 cuộc tấn công mạng vào các hệ thống thông tin tại Việt Nam dẫn đến sự cố (553 cuộc Phishing, 280 cuộc Deface, 223 cuộc Malware), đã giảm 51,4% với 4 tháng đầu năm 2019.

Đạt được những kết quả trên cho thấy việc nâng cao nhận thức, kỹ năng về đảm bảo an toàn, an ninh mạng cho các cơ quan, tổ chức và người dùng, thông qua các hội nghị, hội thảo cũng như các chương trình tập huấn, diễn tập. Bên cạnh đó, các quy định, chế tài pháp luật đã đầy đủ và có tính răn đe hơn như sự ra đời của Luật An ninh mạng có hiệu lực từ ngày 01/01/2019. Sự phối hợp và

tuân thủ của các tổ chức Internet lớn trên thế giới với luật pháp Việt Nam cũng tốt hơn. Đặc biệt, nhận thức về ATTT của tổ chức, cá nhân đã được nâng cao, các biện pháp phòng vệ chủ động đã tốt hơn, công tác đánh giá an toàn thông tin được thực hiện nhiều hơn.

Trong Chỉ thị 01 về định hướng phát triển ngành TT&TT năm 2020, Bộ trưởng Bộ TT&TT đã nhấn mạnh, an toàn, an ninh mạng là điều kiện tiên quyết để phát triển Chính phủ điện tử và chuyển đổi số, do đó phải đi trước một bước. Chỉ thị 01 cũng nêu rõ các chỉ tiêu cần đạt được trong năm 2020 của lĩnh vực an toàn, an ninh mạng như: 100% cơ quan, tổ chức tại Việt Nam triển khai bảo vệ an toàn, an ninh mạng theo mô hình 4 lớp; 100% bộ, ngành, địa phương triển khai các giải pháp điều hành, giám sát an toàn, an ninh mạng, phòng chống mã độc tập trung, kết nối chia sẻ thông tin với Trung tâm giám sát an toàn không gian mạng quốc gia của Bộ TT&TT...

II. Các hành vi vi phạm pháp luật trên không gian mạng

1. Spam, tin giả trên mạng xã hội, thư điện tử

1.1. Spam

Spam hay còn gọi là tin rác, là viết tắt tắt của Stupid Pointless Annoying Messages, từ này có ý nghĩa là những thông điệp vô nghĩa và gây phiền toái cho người nhận, được gửi đến nhiều người dùng với cùng một nội dung [1].

Thuật ngữ spam lần đầu xuất hiện vào năm 1978, khi một người đàn ông gửi thư có nội dung y hệt nhau đến 393 người cùng lúc để quảng cáo sản phẩm mới của mình. Ngày nay, spam xuất hiện trên nhiều phương tiện như spam chat, spam tin tức, spam tin nhắn, spam trong forum, spam trên những mạng xã hội.

1.2. Tin giả

Theo định nghĩa của từ điển Collins, tin giả là “những thông tin sai sự thật, thường là tin giật gân, được phát tán dưới vỏ bọc tin tức”.

Tin giả được tạo ra bằng nhiều hình thức tinh vi. Đặc biệt, hiện nay nhiều đối tượng đã sử dụng CNTT làm giả tiếng, giả hình, giả video để tạo ra tin giả.

- Giả hình: Công nghệ cắt ghép tạo hình ảnh người giả y như thật để tạo ra tin tức giả, nhiều người nổi tiếng đã là nạn nhân. Và nguy hại hơn nếu họ cắt ghép với hình ảnh những chính trị gia, người có uy tín cộng đồng để tạo dư luận giả.

- Giả tiếng: Sử dụng công nghệ TTP (công cụ chuyển văn bản thành tiếng nói - text to speech) để tạo ra các cuộc gọi tự động với giọng robot thu sẵn. Từ nhiều năm trước đã có những người sử dụng công nghệ này để thay họ đọc thông tin, tin tức do họ "xào nấu" ra. Hiện nhiều người đang dùng công nghệ này cho các chương trình trên YouTube.

- Giả video: Thực hiện bằng cách cắt ghép hình ảnh người dẫn chương trình lồng vào dẫn bản tin giả. Clip giả nhưng có người dẫn chương trình sống động như thật. Loại hình ảnh giả này "buộc" người xem nghĩ đó là những thông tin thật vì có hình ảnh quen mặt của người dẫn chương trình truyền hình.

Tin giả có thể được tạo và lan truyền nhằm các mục đích sau:

- Chính trị: Tin giả được lợi dụng vào các âm mưu chính trị và làm rối loạn XH.

- Thương mại: Ngày càng nhiều người biết cách tận dụng công cụ hiện đại, những nền tảng mạng xã hội để phát tán thông tin giả. Số lượng tin giả đối với doanh nghiệp, kinh doanh cũng tăng lên tỷ lệ thuận với tin giả trong các lĩnh vực khác nói chung. Các cách thức phát tán tin giả với doanh nghiệp phổ biến như, đối thủ cạnh tranh sử dụng tin giả để tấn công phía bên kia, dùng những cách thức để bôi xấu về những sự cố đã từng xảy ra trong quá khứ và khi một sự cố vừa xảy ra thì họ sẽ tìm mọi cách để họ nhân rộng sự lên. Hay những tin giả hoàn toàn không có thật liên quan đến vấn đề kinh doanh, vấn đề quan hệ cá nhân của những cán bộ cấp cao, vấn đề bằng cấp, đầu tư mờ ám, liên quan đến nguồn tiền bất hợp pháp có rất nhiều cách thức để làm ảnh hưởng đến một doanh nghiệp, đối thủ. Tin giả bịa đặt để gây bức xúc, tâm lý "tăng tương tác, tăng bán hàng" đã khiến một bộ phận bán hàng trực tuyến chủ động tạo và lan truyền tin giả với mục đích kinh tế hết sức rõ ràng.

1.3. Xử lý hành vi tạo và lan truyền tin giả:

Nghị định 15 có hiệu lực từ ngày 15-4-2020 thay thế cho Nghị định 174/2013/NĐ-CP ngày 13-11-2013 về xử phạt vi phạm hành chính trong lĩnh vực bưu chính, viễn thông, công nghệ thông tin và tần số vô tuyến điện. Một nội dung đáng chú ý trong Nghị định 15 đó là quy định rõ hơn về hành vi vi phạm và trách nhiệm sử dụng dịch vụ mạng xã hội, kèm theo là mức xử phạt vi phạm hành chính đối với các hành vi tung thông tin giả mạo, gây hoang mang dư luận trên mạng XH.

- Điều 101, Nghị định 15 quy định phạt tiền từ 10-20 triệu đồng đối với hành vi lợi dụng mạng xã hội để cung cấp, chia sẻ thông tin giả mạo, thông tin sai sự thật, xuyên tạc, vu khống, xúc phạm uy tín của cơ quan, tổ chức, danh dự, nhân phẩm của cá nhân; cung cấp, chia sẻ thông tin bịa đặt, gây hoang mang trong nhân dân, kích động bạo lực, tội ác, tệ nạn xã hội, đánh bạc hoặc phục vụ đánh bạc.

- Nghị định 15 quy định rất cụ thể các hành vi vi phạm về chống thư rác, tin nhắn rác và cung cấp dịch vụ nội mạng. Mức phạt lên đến 80 triệu đồng đối với hành vi gửi hoặc phát tán thư điện tử rác, tin nhắn rác, phần mềm độc hại (tăng cao so với mức xử phạt được quy định tại Nghị định 174/2013/NĐ-CP chỉ từ 40-50 triệu đồng). Riêng đối với hành vi không ngăn chặn, thu hồi số thuê bao được dùng để phát tán tin nhắn rác thì mức phạt tiền sẽ từ 180-200 triệu đồng.

Đối với các hành vi kể trên, ngoài phạt tiền còn bị áp dụng thêm các hình thức xử phạt bổ sung, biện pháp khắc phục hậu quả như: đình chỉ hoạt động cung cấp dịch vụ từ 1-3 tháng; tước quyền sử dụng mã số quản lý, tên định danh từ 1-3 tháng; buộc thu hồi đầu số, kho số viễn thông.

Ngoài phạt tiền, người vi phạm còn bị buộc áp dụng các biện pháp khắc phục hậu quả: gỡ bỏ thông tin sai sự thật, gây nhầm lẫn hoặc thông tin vi phạm pháp luật do thực hiện hành vi vi phạm.

Theo thông tin từ đại diện Bộ Công an tại cuộc họp báo Chính phủ thường kỳ tháng 1-2020, liên quan đến việc xử lý người dân đăng tin sai lệch về tình hình dịch bệnh viêm đường hô hấp do chủng mới của vi rút Corona, Bộ đã chỉ đạo các đơn vị, địa phương vào cuộc đấu tranh, triệu tập các đối tượng, xử lý, yêu cầu cam kết gỡ bỏ, căn cứ theo Khoản 3, Nghị định của Chính phủ quy định

về xử phạt trong lĩnh vực bưu chính, viễn thông và quy định trong việc loan tin đồn sai qua mạng, xử phạt vi phạm hành chính khoảng 800 người.

2. Đăng tải các thông tin độc hại vi phạm ANQG, trật tự ATXH

Theo Điều 8 Luật An ninh mạng (2018), các hành vi bị nghiêm cấm bao gồm:

1. Sử dụng không gian mạng để thực hiện hành vi sau đây:

a) Hành vi quy định tại khoản 1 Điều 18 của Luật này;

b) Tổ chức, hoạt động, câu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam;

c) Xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc;

d) Thông tin sai sự thật gây hoang mang trong Nhân dân, gây thiệt hại cho hoạt động kinh tế - xã hội, gây khó khăn cho hoạt động của cơ quan nhà nước hoặc người thi hành công vụ, xâm phạm quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác;

đ) Hoạt động mại dâm, tệ nạn xã hội, mua bán người; đăng tải thông tin dâm ô, đồi trụy, tội ác; phá hoại thuần phong, mỹ tục của dân tộc, đạo đức xã hội, sức khỏe của cộng đồng;

e) Xúi giục, lôi kéo, kích động người khác phạm tội.

2. Thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; gây sự cố, tấn công, xâm nhập, chiếm quyền điều khiển, làm sai lệch, gián đoạn, ngưng trệ, tê liệt hoặc phá hoại hệ thống thông tin quan trọng về an ninh quốc gia.

3. Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; phát tán chương trình tin học gây hại cho hoạt động của mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, phương tiện điện tử; xâm nhập trái phép vào mạng viễn thông, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu, phương tiện điện tử của người khác.

4. Chống lại hoặc cản trở hoạt động của lực lượng bảo vệ an ninh mạng; tấn công, vô hiệu hóa trái pháp luật làm mất tác dụng biện pháp bảo vệ an ninh mạng.

5. Lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân hoặc để trục lợi.

6. Hành vi khác vi phạm quy định của Luật này.

Theo Khoản 1, Điều 16. Thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam bao gồm:

a) Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;

b) Chiến tranh tâm lý, kích động chiến tranh xâm lược, chia rẽ, gây thù hận giữa các dân tộc, tôn giáo và nhân dân các nước;

c) Xúc phạm dân tộc, quốc kỳ, quốc huy, quốc ca, vĩ nhân, lãnh tụ, danh nhân, anh hùng dân tộc.

Theo Khoản 2, Điều 16. Thông tin trên không gian mạng có nội dung kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng bao gồm:

a) Kêu gọi, vận động, xúi giục, đe dọa, gây chia rẽ, tiến hành hoạt động vũ trang hoặc dùng bạo lực nhằm chống chính quyền nhân dân;

b) Kêu gọi, vận động, xúi giục, đe dọa, lôi kéo tụ tập đông người gây rối, chống người thi hành công vụ, cản trở hoạt động của cơ quan, tổ chức gây mất ổn định về an ninh, trật tự.

3. Chiếm đoạt tài khoản mạng xã hội

Một số hình thức, thủ đoạn được các đối tượng sử dụng để chiếm đoạt mạng xã hội như sau:

- Hình thức Phishing: Đây là hình thức chiếm đoạt một tài khoản facebook phổ biến nhất hiện nay và cho đến bây giờ nó vẫn là cách được hacker sử dụng nhiều nhất. Không riêng gì facebook mà hầu hết các loại website nào mà có account đăng nhập đều sử dụng được hình thức này. Sau đây là nguyên lý hoạt động:

+ Kẻ tấn công sẽ phát tán một đường link ở nhiều nơi và nhất là trên Facebook với những tiêu đề gây sốc như: Click vào đây để xem xxx .... gây kích thích và sự tò mò cho người xem.

+ Khi người dùng click vào đường dẫn sẽ được đưa đến một website có giao diện giống 100% facebook và yêu cầu bạn đăng nhập tài khoản của mình. Đây không phải là trang facebook mà chỉ là một website có giao diện giống facebook. Nếu người dùng đăng nhập tài khoản facebook vào thì tất cả tài khoản, mật khẩu sẽ được gửi về email hay sever của kẻ tấn công, như vậy các hacker đã dễ dàng lấy được nick facebook của người dùng.

- Dò mật khẩu: Sau phishing facebook thì đây là một hình thức phổ biến tuy xác xuất thành công không cao nhưng không thể không nói đến nó vì có nhiều người dùng sử dụng những mật khẩu quá đơn giản kiểu như: 123456 , matkhau, số điện thoại , họ và tên....Đây là những sai lầm ở phía người dùng khi đặt mật khẩu facebook. Hacker sử dụng những phần mềm chuyên dò pass để đi dò mật khẩu nick facebook của người dùng. Với cách này bản chất nó không phải hack mà là mò pass facebook nhưng một khi bị mất mật khẩu thì đồng nghĩa với việc bạn bị mất tài khoản.

- Sử dụng trojan, Keylog: Kẻ tấn công sẽ chèn một đoạn mã vào một ứng dụng,tập tin nào đó rồi gửi thông qua inbox, comment trên facebook hay bất cứ đâu. Khi người dùng click vào đường dẫn đó thì ứng dụng, tập tin đó sẽ được tự động tải về máy, sau đó keylog sẽ ghi lại tất cả những thao tác trên bàn phím của người dùng rồi gửi về cho kẻ tấn công.

- Sử dụng chương trình khuyến mãi - trúng thưởng hay Mini Game: Hacker sẽ giả chương trình trúng thưởng - khuyến mãi trên danh nghĩa của Facebook (trúng thưởng xe máy, ô tô, tiền mặt… có giá trị cao) và yêu cầu người dùng xác nhận bằng cách truy cập vào đường link lạ. Các Mini game trên facebook như: "Bạn giống cầu thủ bóng đá nào?", "Tương lai bạn sẽ kết hôn với ai?", "Ai là người quan

tâm bạn nhất?",... Cũng được những kẻ này sử dụng để chiếm lấy tài khoản facebook bằng cách buộc người chơi đăng nhập mật khẩu trước khi tham gia.

- Lỗ hổng bảo mật facebook: Là hình thức tấn công nick facebook mạng tên "3 Friends". Đây là hình thức lấy lại mật khẩu của facebook thông qua việc sử dụng 3 người bạn facebook bất kì trong danh sách bạn bè. Ví dụ khi bạn quên mật khẩu thì bạn có thể gửi yêu cầu để facebook gửi 3 mã code về cho 3 người bạn này.

Kẻ tấn công chiếm đoạt tài sản mạng xã hội nhằm các mục đích sau:

- Lừa đảo, chiếm đoạt tài sản.
- Hack nick facebook vì những thù hằn của cá nhân.

4. Chiếm quyền giám sát Camera IP

Trong những năm gần đây, thị trường Camera IP wifi phát triển nhanh chóng do nhu cầu sử dụng của người dân tăng mạnh. Những thiết bị này chủ yếu có nguồn gốc xuất xứ từ Trung Quốc, Đài Loan với giá thành rất rẻ. Tuy nhiên, đi kèm theo đó là các rủi ro và nguy cơ bảo mật. Đã có nhiều gia đình, cá nhân bị lộ clip riêng tư do camera giám sát bị các đối tượng xấu chiếm quyền giám sát. Một số thủ đoạn:

Cách thứ nhất: Tấn công trực tiếp vào thiết bị Camera bằng cách Quét (Scan) IP và Port của Camera rồi sau đó Hacker tìm cách xâm nhập vào hệ thống để xem hình ảnh, video trái phép. Cách này rất phổ biến, bởi đa số người dùng camera hiện tại thường sử dụng Password mặc định của nhà cung cấp.

Cách thứ hai: Hacker sẽ dùng một phần mềm gián điệp cài trên Camera quan sát để tạo thành một mạng Botnet sử dụng trong một hình thức tấn công nổi tiếng đó là DDOS.

Ví dụ: Ngày 28/12/2019, video được đăng trên một trang web phim người lớn được cho là quay lại cảnh sinh hoạt của ca sĩ Văn Mai Hương. Những video này được ghi lại từ năm 2015 qua camera IP (camera giám sát) trong căn hộ của nữ ca sĩ.

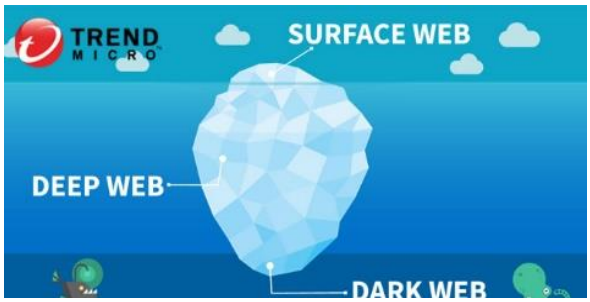
5. Lừa đảo chiếm đoạt tài sản

Kịch bản lừa đảo thông báo trúng thưởng với giải thưởng cực lớn đang quay trở lại hoành hành trên Facebook. Sau khi chiếm đoạt tài khoản Facebook cá nhân, nhiều đối tượng còn tung ra nhiều chiêu trò để lừa đảo khiến nhiều người dùng mất đi một khoản tiền không hề nhỏ. Ngay sau khi có tài khoản đã được đánh cắp, đối tượng sẽ thực hiện ngay việc chat với bạn bè/người thân hỏi thăm về sức khỏe, công việc và sau đó nhờ nhận hộ một số tiền chuyển từ nước ngoài về. Nạn nhân không biết tài khoản Facebook kia đã bị tấn công nên tin tưởng và sẵn sàng giúp đỡ.

Không chỉ vậy, nạn nhân còn có nguy cơ bị tấn công lấy tài khoản ngân hàng thông qua hình thức tấn công phishing. Sau khi thống nhất số tiền sẽ chuyển, đối tượng lừa đảo dùng một số điện thoại từ nước ngoài sẽ gửi 1 tin nhắn giả mạo thông báo từ Western Union đến số điện thoại của nạn nhân với nội dung đề nghị truy cập đường link trong tin nhắn SMS và xác nhận để có thể nhận được tiền Western Union.

Nạn nhân không biết đây là trang web phishing (một hình thức lừa đảo giả mạo các tổ chức uy tín như ngân hàng) nên đã nhập các thông tin tài khoản, mật khẩu internet banking vào trang web giả mạo rồi gửi đi và đối tượng lừa đảo sẽ nhận được. Từ đó, đối tượng lừa đảo dùng thông tin internet banking vừa chiếm được từ nạn nhân để thực hiện giao dịch qua cổng thanh toán trực tuyến VTC Pay và cổng thanh toán VNPAY.

6. Deep web và Dark web



Hình 10. Surface web, Deep web và Dark web

6.1. Deep web

Thuật ngữ Internet và World Wide Web thường được sử dụng thay cho nhau, nhưng thực ra chúng không phải là một. Internet đề cập đến một mạng lưới rộng lớn của các mạng, hàng triệu kết nối máy tính trên khắp thế giới, nơi bất kỳ máy tính nào cũng có thể giao tiếp với nhau, miễn là chúng được kết nối Internet. World Wide Web là một mô hình chia sẻ thông tin, được xây dựng trên Internet, sử dụng giao thức HTTP, các trình duyệt như Chrome, Firefox và các trang web để chia sẻ thông tin. Web là một phần to lớn của Internet nhưng không phải là thành phần duy nhất. Ví dụ: email, tin nhắn không phải là một phần của web nhưng là một phần của Internet.

Web trên bề mặt (tiếng Anh: Surface web): Theo tạp chí PC Magazine, web bề mặt là một phần web có sẵn cho công chúng, hoàn chỉnh với những liên kết được công cụ tìm kiếm lập chỉ mục. BrightPlanet, một dịch vụ web thông minh, xác định web bề mặt chỉ chứa những trang web được lập chỉ mục và có thể được tìm kiếm bởi các công cụ tìm kiếm phổ biến như Google, Bing, Yahoo. Đôi khi, chúng còn được gọi là web hữu hình. Web bề mặt thường bao gồm những trang web có tên miền kết thúc bằng .com, .org, .net, .vn hoặc các biến thể tương tự. Nội dung của các trang web này không yêu cầu bất kỳ cấu hình đặc biệt nào để truy cập.

Web chìm (tiếng Anh: Deep web) hay còn gọi là web ẩn (invisible web, undernet, hay hidden web) là từ dùng để chỉ các trang hoặc nội dung trên thế giới mạng World Wide Web không thuộc về Web nổi (surface Web). Chúng gồm những trang không được đánh dấu, chỉ mục (index) và không thể tìm kiếm được khi dùng các công cụ tìm kiếm thông thường.

Web chìm bao gồm nhiều ứng dụng rất phổ biến như web mail và ngân hàng trực tuyến nhưng nó cũng bao gồm các dịch vụ mà người dùng phải trả tiền, và được bảo vệ bởi một paywall, như video theo yêu cầu, một số tạp chí và báo chí trực tuyến, và nhiều hơn nữa. Nó bao gồm email trong tài khoản Gmail, các bản kê ngân hàng trực tuyến, mạng nội bộ, tin nhắn trực tiếp qua Twitter,

hình ảnh được đánh dấu riêng tư khi tải lên Facebook. Chính phủ, các nhà nghiên cứu và các công ty lưu trữ dữ liệu thô không thể tiếp cận được với công chúng. Nội dung này được lưu trữ trên các trang web động (được xây dựng dựa trên thông tin truy vấn) và những trang bị khóa, những trang cá nhân không liên kết ra bên ngoài. Theo Trend Micro, một phần quan trọng của Deep Web là được dành riêng cho những blog cá nhân hoặc chính trị, các trang tin tức, diễn đàn thảo luận, các trang web tôn giáo và thậm chí đài phát thanh.

6.2. Dark web

Mỗi thiết bị được kết nối với Internet đều có địa chỉ IP (Internet protocol) duy nhất. Tên và địa chỉ vật lý của một người có thể có được thông qua một nhà cung cấp dịch vụ Internet với sự cho phép hợp pháp, còn IP cho phép bất cứ ai xác định vị trí của máy tính được kết nối. Do đó, các bên liên quan sẽ dễ dàng tìm được một người sử dụng Internet cụ thể.

Với mong muốn ẩn danh - đặc biệt là chính phủ khi tìm cách bảo vệ những thông tin, mạng lưới tình báo nhạy cảm - đã dẫn đến sự ra đời và phát triển của The Onion Router (Tor) do đội ngũ nhân viên phòng thí nghiệm nghiên cứu Hải Quân Hoa Kỳ tạo ra. Tên Onion (củ hành) bắt nguồn từ việc bạn phải lột ra nhiều "lớp vỏ" để có thể tìm thấy danh tính thật sự của người dùng.

Tor, được phát hành miễn phí cho người dùng vào năm 2004, cung cấp sự riêng tư bằng cách mã hóa và điều hướng lưu lượng truy cập thông qua một sê-ri "đường hầm ảo (virtual tunnel)", phân phối các giao dịch qua nhiều máy tính ngẫu nhiên trên Internet, do đó, không một máy tính nào liên kết người dùng đến cơ sở hoặc điểm đến của họ. Không giống như những trang web bề mặt (kết thúc bằng .com, .org, .net hoặc các biến thể tương tự), các trang Tor kết thúc bằng .onion và chỉ có thể được mở bằng phần mềm Tor.

Dark web (tạm dịch: web tối) là những nội dung mạng World Wide Web không thể truy cập bằng những cách thông thường mà phải sử dụng các phần mềm chuyên biệt [3]. Dark web là một phần nhỏ của deep web, một thế giới mạng mà các công cụ tìm kiếm như Google hay Bing không hiển thị ra.

Một số hoạt động thường thấy ở Dark Web:

- Chợ đen: Nhiều hoạt động thương mại bất hợp pháp diễn ra trên Dark web, ví dụ như: buôn bán tiền giả, thẻ ngân hàng hay tài khoản mạng bị đánh cắp, súng, ma túy và các chất kích thích, các sản phẩm không rõ nguồn gốc khác.

- Khủng bố: Vì tính ẩn danh cao, nhiều tổ chức tội phạm khủng bố như IS sử dụng không gian Dark web để phát tán các nội dung đến người dùng. Nói đến khủng bố thì không chỉ là IS mà còn có các tổ chức Mafia khác sử dụng mạng lưới này, đã từng có trường hợp chúng nhận hợp đồng thanh toán một người và hợp đồng đó đã ở trạng thái được thực thi.

- Khiêu dâm: Khiêu dâm trẻ em, ngược đãi hoặc làm tình với động vật, phát tán video quay lén là những nội dung hiện hữu trên dark web. Các nội dung này đều bị các tổ chức bảo vệ trẻ em cũng như các nước trên thế giới lên án và cố gắng dẹp bỏ

- Lừa đảo: Không hiếm những trường hợp lừa tiền hoặc thanh toán người khác trên Dark Web được thực thi.

III. PHÒNG, CHỐNG VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG

1. Cơ sở pháp lý

1.1. Bộ luật Hình sự năm 2015

a. Hoàn cảnh ra đời

Ngày 27/11/2015, tại Kỳ họp thứ 10, Quốc hội khóa XIII đã thông qua Bộ luật Hình sự. Ngày 20/6/2017, tại Kỳ họp thứ 2, Quốc hội khóa XIV đã thông qua Luật sửa đổi, bổ sung một số điều của Bộ luật Hình sự số 100/2015/QH13. BLHS số 100/2015/QH13 được sửa đổi, bổ sung năm 2017 đã đánh dấu một bước tiến quan trọng, tạo cơ sở pháp lý vững chắc cho cuộc đấu tranh phòng, chống tội phạm có hiệu quả; góp phần bảo vệ chủ quyền, an ninh của đất nước, bảo vệ chế độ, bảo vệ quyền con người, quyền công dân, lợi ích của Nhà nước và tổ chức, bảo vệ và thúc đẩy kinh tế thị trường xã hội chủ nghĩa phát triển đúng hướng, tạo môi trường xã hội và môi trường sinh thái an toàn, lành mạnh cho mọi người dân, đồng thời đáp ứng yêu cầu hội nhập quốc tế của nước ta.

b. Hiệu lực thi hành

Bộ luật Hình sự năm 2015, sửa đổi bổ sung năm 2017 (Gọi tắt là Bộ luật Hình sự) có hiệu lực thi hành từ ngày 01/01/2018.

c. Bố cục của Bộ luật Hình sự

Bộ luật hình sự gồm 26 Chương và 526 Điều, bao gồm:

- Chương I. Điều khoản cơ bản (Điều 01 – Điều 04).
- Chương II. Hiệu lực của bộ luật hình sự (Điều 05 – Điều 07)
- Chương III. Tội phạm (Điều 8 – Điều 19).
- Chương IV. Những trường hợp loại trừ trách nhiệm hình sự (Điều 20– Điều 26).
- Chương V. Thời hiệu truy cứu trách nhiệm hính sự, miễn trách nhiệm hình sự (Điều 27 – Điều 29).
- Chương VI. Hình phạt (Điều 30 – Điều 45).
- Chương VII. Các biện pháp tư pháp (Điều 46 – Điều 49).
- Chương VIII. Quyết định hình phạt (Điều 50 – Điều 59).
- Chương IX. Thời hiệu thi hành bản án, miễn chấp hành hình phạt, giảm thời hạn chấp hành hình phạt (Điều 60 – Điều 68).
- Chương X. Xóa án tích (Điều 69– Điều 73).
- Chương XI. Những quy định đối với pháp nhân thương mại phạm tội (Điều 74 – Điều 89).
- Chương XII. Những quy định đối với người dưới 18 tuổi phạm tội (Điều 90 – Điều 107).
- Chương XIII. Các tội xâm phạm an ninh quốc gia (Điều 108 – Điều 122).
- Chương XIV. Các tội phạm xâm phạm tính mạng, sức khỏe, nhân phẩm, danh dự của con người (Điều 123 – Điều 156).

- Chương XV. Các tội xâm phạm quyền tự do của con người, quyền tự do, dân chủ của công dân (Điều 157 – Điều 167).

- Chương XVI. Các tội xâm phạm sở hữu (Điều 168 – Điều 180).

- Chương XVII. Các tội phạm chế độ hôn nhân và gia đình (Điều 181 – Điều 187).

- Chương XVIII. Các tội xâm phạm trật tự quản lý kinh tế (Điều 188 – Điều 234).

- Chương XIX. Các tội phạm về môi trường (Điều 235 – Điều 246).

- Chương XX. Các tội phạm về ma túy (Điều 247 – Điều 259).

- Chương XXI. Các tội xâm phạm an toàn công cộng, trật tự công cộng (Điều 260 – Điều 329).

- Chương XXII. Các tội xâm phạm trật tự quản lý hành chính (Điều 330 – Điều 351).

- Chương XXIII. Các tội phạm về chức vụ (Điều 352 – Điều 366).

- Chương XXIV. Các tội xâm phạm hoạt động tư pháp (Điều 367– Điều 391).

- Chương XXV. Các tội xâm phạm nghĩa vụ, trách nhiệm của quân nhân và trách nhiệm của người phối thuộc với quân đội trong chiến đấu, phục vụ chiến đấu (Điều 392– Điều 420).

- Chương XXVI. Các tội phá hoại hòa bình, chống loài người và tội phạm chiến tranh (Điều 421– Điều 426).

Trong đó các Điều khoản trong luật thực hiện với các hành vi vi phạm pháp luật trên không gian mạng được quy định tại **Mục 2. Tội phạm trong lĩnh vực công nghệ thông tin, mạng viễn thông** Chương XII gồm các Điều 285 đến 294.

+ Điều 285. Tội sản xuất, mua bán, trao đổi hoặc tặng cho công cụ, thiết bị, phần mềm để sử dụng vào mục đích trái pháp luật.

+ Điều 286. Tội phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử.

+ Điều 287. Tội cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử.

+ Điều 288. Tội đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông.

+ Điều 289. Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác.

+ Điều 290. Tội sử dụng mạng máy tính, mạng viễn thông, phương tiện điện tử thực hiện hành vi chiếm đoạt tài sản.

+ Điều 291. Tội thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng.

+ Điều 292. Tội cung cấp dịch vụ trái phép trên mạng máy tính, mạng viễn thông

+ Điều 293. Tội sử dụng trái phép tần số vô tuyến điện dành riêng cho mục đích cấp cứu, an toàn, tìm kiếm, cứu hộ, cứu nạn, quốc phòng, an ninh.

+ Điều 294. Tội cố ý gây nhiễu có hại.

1.2. Luật An toàn thông tin 2015

a. Hoàn cảnh ra đời

Hiện nay, mạng Internet đã trở thành công cụ trung tâm để phát triển nền kinh tế và xã hội của mọi quốc gia. Đối với Việt Nam, mạng internet cũng được coi là công cụ, phương tiện quan trọng để thực hiện mục tiêu đưa Việt Nam trở thành nước công nghiệp hóa, hiện đại hóa, phát triển mạnh trong một thế giới cạnh tranh và toàn cầu hóa. Vì vậy, Việt Nam cần có các quy định pháp lý về an toàn thông tin để nội luật hóa các điều ước quốc tế mà Việt Nam là thành viên; phù hợp với thông lệ quốc tế, bảo đảm ATTT, tạo môi trường bình đẳng cho các tổ chức, doanh nghiệp hoạt động sản xuất, kinh doanh tại Việt Nam.

b. Hiệu lực thi hành

Luật An toàn thông tin có hiệu lực thi hành từ ngày 01/7/2016.

c. Bố cục của Luật An toàn thông tin

Luật An toàn thông tin mạng gồm 08 Chương và 54 Điều, bao gồm:

- Chương I. Những quy định chung (Điều 01 – Điều 08) Chương này quy định về phạm vi điều chỉnh, đối tượng áp dụng, giải thích từ ngữ, nguyên tắc bảo đảm an toàn thông tin mạng, chính sách của nhà nước, hợp tác quốc tế, những hành vi bị cấm trong hoạt động an toàn thông tin mạng và xử lý vi phạm pháp luật về an toàn thông tin mạng.

- Chương II. Bảo đảm an toàn thông tin mạng (Điều 09 – Điều 29) Chương này quy định 04 mục: Bảo vệ thông tin mạng; Bảo vệ thông tin cá nhân; Bảo vệ hệ thống thông tin; Ngăn chặn xung đột thông tin trên mạng.

- Chương III. Mật mã dân sự (Điều 30 – Điều 36) Chương này quy định các nội dung liên quan đến sản phẩm, dịch vụ mật mã dân sự và các hoạt động có liên quan đến kinh doanh sản phẩm, dịch vụ mật mã dân sự.

- Chương IV. Tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng (Điều 37 – Điều 39) Chương này quy định các nội dung về tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng; quản lý tiêu chuẩn, quy chuẩn kỹ thuật an toàn thông tin mạng và chứng nhận, công bố hợp quy và đánh giá, kiểm định an toàn thông tin mạng.

Chương V. Kinh doanh trong lĩnh vực an toàn thông tin mạng (Điều 40 – Điều 48), gồm 02 mục: Giấy phép kinh doanh sản phẩm an toàn thông tin mạng; Quản lý nhập khẩu sản phẩm an toàn thông tin mạng.

Đây là lĩnh vực rất mới, hành lang pháp lý cho hoạt động kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng còn chưa đầy đủ, nên Luật an toàn thông tin mạng hướng tới việc hoàn thiện hành lang pháp lý đảm bảo thông thoáng, công bằng, phù hợp với thông lệ quốc tế, thúc đẩy thị trường phát triển bền vững

- Chương VI. Phát triển nguồn nhân lực an toàn thông tin mạng (Điều 49 – Điều 50). Chương này quy định về các hoạt động đào tạo, bồi dưỡng nghiệp vụ về an toàn thông tin mạng, văn bằng, chứng chỉ đào tạo về an toàn thông tin mạng tại Việt Nam, thể hiện đúng đường lối chủ trương của Đảng và Nhà nước ta trong thời gian vừa qua.

- Chương VII. Quản lý nhà nước về an toàn thông tin mạng (Điều 51 – Điều 52). Hệ thống hoá thẩm quyền và trách nhiệm của cơ quan quản lý nhà nước các cấp, qua đó giúp các cơ quan này có thể tham chiếu một cách hệ thống, cơ bản về các quyền hạn và trách nhiệm của mình trong quá trình đảm bảo an

toàn thông tin bên cạnh việc xác định các nội dung cụ thể xoay quanh nội dung quản lý nhà nước về an toàn thông tin mạng, bao gồm các hoạt động xây dựng chiến lược, quy hoạch, kế hoạch; hoạt động xây dựng và hoàn thiện thể chế; tổ chức thực thi các văn bản; quản lý nhà nước trên các lĩnh vực; hoạt động thanh tra kiểm tra; hợp tác quốc tế...

- Chương VIII. Điều khoản thi hành (Điều 53 – Điều 54) quy định về hiệu lực thi hành.

1.3. Luật An ninh mạng 2018

a. Hoàn cảnh ra đời

Trước yêu cầu cấp bách của tình hình an ninh mạng trong bảo vệ an ninh quốc gia, bảo đảm trật tự an toàn xã hội; khắc phục những tồn tại, hạn chế cơ bản trong công tác bảo vệ an ninh mạng; thể chế hóa đầy đủ, kịp thời các chủ trương, đường lối của Đảng về an ninh mạng; bảo đảm sự phù hợp với quy định của Hiến pháp năm 2013 về quyền con người, quyền cơ bản của công dân và bảo vệ Tổ quốc. Ngày 12/6/2018, Quốc hội khóa XIV, kỳ họp thứ 5 đã thông qua dự thảo Luật An ninh mạng với 86,86% đại biểu đồng ý.

b. Hiệu lực thi hành

Luật An ninh mạng có hiệu lực thi hành từ ngày 01/01/2019.

c. Bố cục của Luật An ninh mạng

Luật An ninh mạng gồm 07 Chương, 43 Điều. Bố cục của Luật cụ thể như sau:

Chương I. Những quy định chung, gồm 9 điều, (từ Điều 1 đến Điều 9) quy định về phạm vi điều chỉnh; giải thích từ ngữ; chính sách của Nhà nước về an ninh mạng; nguyên tắc bảo vệ an ninh mạng; biện pháp bảo vệ an ninh mạng; bảo vệ không gian mạng quốc gia; hợp tác quốc tế về an ninh mạng; các hành vi bị nghiêm cấm về an ninh mạng; xử lý vi phạm pháp luật về an ninh mạng.

Chương II. Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, gồm 6 điều (từ Điều 10 đến Điều 15), quy định về hệ thống thông tin quan trọng về an ninh quốc gia; thẩm định an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; đánh giá điều kiện an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; kiểm tra an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; giám sát an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; ứng phó, khắc phục sự cố an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia.

Chương III. Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng, gồm 7 điều (từ Điều 16 đến Điều 22), quy định về phòng ngừa, xử lý thông tin trên không gian mạng có nội dung tuyên truyền chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam; kích động gây bạo loạn, phá rối an ninh, gây rối trật tự công cộng; làm nhục, vu khống; xâm phạm trật tự quản lý kinh tế; phòng, chống gián điệp mạng; bảo vệ thông tin thuộc bí mật nhà nước, bí mật công tác, bí mật kinh doanh, bí mật cá nhân, bí mật gia đình và đời sống riêng tư trên không gian mạng; phòng, chống hành vi sử dụng không gian mạng, công nghệ thông tin,

phương tiện điện tử để vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội; phòng, chống tấn công mạng; phòng, chống khủng bố mạng; phòng ngừa, xử lý tình huống nguy hiểm về an ninh mạng; đấu tranh bảo vệ an ninh mạng.

Chương IV. Hoạt động bảo vệ an ninh mạng, gồm 7 điều (từ Điều 23 đến Điều 29), quy định về triển khai hoạt động bảo vệ an ninh mạng trong cơ quan nhà nước, tổ chức chính trị ở trung ương và địa phương; kiểm tra an ninh mạng đối với hệ thống thông tin của cơ quan, tổ chức không thuộc Danh mục hệ thống thông tin quan trọng về an ninh quốc gia; bảo vệ an ninh mạng đối với cơ sở hạ tầng không gian mạng quốc gia; cổng kết nối mạng quốc tế; bảo đảm an ninh thông tin trên không gian mạng; nghiên cứu, phát triển an ninh mạng; nâng cao năng lực tự chủ về an ninh mạng; bảo vệ trẻ em trên không gian mạng.

Chương V. Bảo đảm hoạt động bảo vệ an ninh mạng, gồm 6 điều (từ Điều 30 đến Điều 35), quy định về lực lượng bảo vệ an ninh mạng; bảo đảm nguồn nhân lực bảo vệ an ninh mạng; tuyển chọn, đào tạo, phát triển lực lượng bảo vệ an ninh mạng; giáo dục, bồi dưỡng kiến thức, nghiệp vụ an ninh mạng; phổ biến kiến thức về an ninh mạng; kinh phí bảo vệ an ninh mạng.

Chương VI. Trách nhiệm của cơ quan, tổ chức, cá nhân, gồm 7 điều (từ Điều 36 đến Điều 42), quy định về trách nhiệm của Bộ Công an; trách nhiệm của Bộ Quốc phòng; trách nhiệm của Bộ Thông tin và Truyền thông; trách nhiệm của Ban Cơ yếu Chính phủ; trách nhiệm của Bộ, ngành, Ủy ban nhân dân cấp tỉnh; trách nhiệm của doanh nghiệp cung cấp dịch vụ trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân sử dụng không gian mạng.

Chương VII. Điều khoản thi hành, gồm 01 điều (Điều 43), quy định về hiệu lực thi hành.

2. Các biện pháp phòng chống vi phạm pháp luật trên không gian mạng

2.1. Thứ nhất: Giáo dục nâng cao nhận thức về bảo vệ chủ quyền quốc gia, các lợi ích và sự nguy hại đến từ không gian mạng.

Ngày nay, quan niệm về lãnh thổ, chủ quyền, biên giới của một quốc gia không chỉ là đất liền, hải đảo, vùng biển và vùng trời, mà cả lãnh thổ không gian mạng, chủ quyền không gian mạng. Theo đó, lãnh thổ không gian mạng là một bộ phận hợp thành lãnh thổ quốc gia, nơi xác định biên giới mạng và thực thi chủ quyền quốc gia trên không gian mạng.

Bảo vệ chủ quyền quốc gia còn là bảo vệ không gian mạng của quốc gia, bao gồm, bảo vệ các hệ thống thông tin; các chủ thể hoạt động trên không gian mạng; hệ thống dữ liệu, tài nguyên mạng; các quy tắc xử lý và truyền số liệu. Đảm bảo quyền bình đẳng trong tham dự quản lý mạng Internet quốc tế; độc lập trong vận hành hạ tầng cơ sở thông tin thuộc lãnh thổ quốc gia; bảo vệ không gian mạng quốc gia không bị xâm phạm và quyền quản trị truyền tải cũng như xử lý số liệu của quốc gia.

Cán bộ, đảng viên và các tầng lớp nhân dân cần nhận thức rõ các nguy cơ đến từ không gian mạng như: tấn công mạng, gián điệp mạng, khủng bố mạng, tội phạm mạng, đặc biệt là nguy cơ chiến tranh mạng đang là thách thức gay gắt

về an ninh, và bảo đảm an ninh mạng đang trở thành trọng tâm ưu tiên của quốc gia. Vì vậy, cần quán triệt các quan điểm của Đảng về phát triển khoa học công nghệ và chiến lược bảo vệ Tổ quốc trong tình hình mới, các định hướng hành động của Việt Nam trong bảo vệ chủ quyền và lợi ích quốc gia trên không gian mạng và nhận thức rõ rằng, đe dọa trên không gian mạng là một trong những mối đe dọa thực tế và nguy hiểm nhất đối với an ninh quốc gia hiện nay.

2.2. Thứ hai: Tuyên truyền, phổ biến, giáo dục các quy định của pháp luật về quản lý không gian mạng.

Phổ biến các điều khoản của Bộ luật Hình sự 2015 (Mục 2, Điều 285-294) liên quan đến lĩnh vực công nghệ thông tin, mạng viễn thông; Nghị định số 72/2013/NĐ-CP ngày 15-7-2013 của Chính phủ và Thông tư số 09/2014/BTTTT ngày 19-8-2014 của Bộ Thông tin và Truyền thông về hoạt động quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử và mạng xã hội, những hành vi bị nghiêm cấm trong sử dụng mạng xã hội.

Tuyên truyền, phổ biến, giáo dục Luật An ninh mạng năm 2018. Luật An ninh mạng được xây dựng nhằm bảo vệ người dùng hợp pháp trên không gian mạng; phòng ngừa, đấu tranh, làm thất bại hoạt động sử dụng không gian mạng xâm phạm an ninh quốc gia, chống Nhà nước, tuyên truyền phá hoại tư tưởng, phá hoại nội bộ, kích động biểu tình, phá rối an ninh trên mạng của các thế lực phản động. Phòng ngừa, ngăn chặn, ứng phó, khắc phục hậu quả của các đợt tấn công mạng, khủng bố mạng và phòng, chống nguy cơ chiến tranh mạng.

Tuyên truyền sâu rộng về những hành vi bị cấm trong Luật An ninh mạng, nhất là các hành vi sử dụng không gian mạng để tuyên truyền chống Nhà nước; tổ chức, hoạt động, cấu kết, xúi giục, mua chuộc, lừa gạt, lôi kéo, đào tạo, huấn luyện người chống Nhà nước; xuyên tạc lịch sử, phủ nhận thành tựu cách mạng, phá hoại khối đại đoàn kết toàn dân tộc, xúc phạm tôn giáo, phân biệt đối xử về giới, phân biệt chủng tộc; thông tin sai sự thật; hoạt động mại dâm, tệ nạn xã hội; phá hoại thuần phong, mỹ tục; xúi giục, lôi kéo, kích động người khác phạm tội; thực hiện tấn công mạng, khủng bố mạng, gián điệp mạng, tội phạm mạng; lợi dụng hoặc lạm dụng hoạt động bảo vệ an ninh mạng để xâm phạm chủ quyền, lợi ích, an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân hoặc để trục lợi.

Các hình thức giáo dục cần được vận dụng đa dạng, phong phú và linh hoạt như: phối hợp giữa cơ quan chức năng với các cơ quan, địa phương, đơn vị, doanh nghiệp, cơ sở giáo dục tổ chức nói chuyện chuyên đề, phổ biến pháp luật; tuyên tuyền Luật An ninh mạng; các cuộc thi tìm hiểu về an toàn thông tin; góp ý xây dựng chương trình giáo dục an toàn thông tin mạng của các cơ sở giáo dục hoặc tham gia biên soạn các tài liệu liên quan đến an toàn thông tin mạng.

2.3. Thứ ba: Bồi dưỡng kỹ năng nhận diện các âm mưu, thủ đoạn tấn công mạng và các hình thái phát sinh trên không gian mạng.

Hoạt động tấn công không gian mạng rất đa dạng và tinh vi như: làm mất kết nối Internet, đánh sập các website của chính phủ, cơ quan, đơn vị, nhà trường, doanh nghiệp; giả mạo các website nhằm lừa đảo; cài gắm vào máy tính cá nhân hoặc lấy tài khoản và mật khẩu; đánh cắp dữ liệu cá nhân (hình ảnh, file,

video); tấn công bằng mã độc (theo tệp đính kèm trong email hoặc ẩn trong quảng cáo Skype); tấn công ẩn danh bằng những phần mềm độc hại (phần mềm diệt virus, các trình duyệt); tấn công qua usb, đĩa CD, địa chỉ IP, server…

Ở mức độ cao hơn, các thế lực thù địch có thể thông qua block cá nhân lôi kéo, kích động các phần tử bất mãn, tập hợp lực lượng, thành lập các tổ chức chống đối như Việt Tân, Chính phủ quốc gia Việt Nam lâm thời, Thanh Niên Dân Chủ,… núp dưới vỏ bọc các tổ chức "xã hội dân sự", "diễn đàn dân chủ" để xuyên tạc cương lĩnh, đường lối, quan điểm, nền tảng tư tưởng của Đảng.

Các thế lực thù địch còn lợi dụng báo điện tử, các website, dịch vụ thư điện tử, mạng xã hội facebook, Zalo, Twitter, diễn đàn,... để phát tán các tài liệu, kêu gọi tuần hành, biểu tình, gây mất ổn định an ninh chính trị, trật tự an toàn xã hội, chống phá chính quyền, chia rẽ mối đoàn kết giữa Đảng và Nhân dân hoặc sử dụng "khoảng trống thông tin" để tấn công vào sự hiếu kỳ của công chúng; làm mới thông tin cũ, bịa đặt thông tin mới để chống phá. Các trang mạng có nhiều nội dung thông tin xấu, độc như Dân Làm Báo, Quan Làm Báo; Boxit, Dân Luận, Chân Dung Quyền Lực…

2.4. Thứ tư: Nâng cao ý thức phòng tránh, tự vệ và sử biện pháp kỹ thuật để khắc phục hậu quả trong trường hợp bị tấn công trên không gian mạng.

Nêu cao ý thức chính trị, trách nhiệm, nghĩa vụ công dân đối với nhiệm vụ bảo vệ không gian mạng quốc gia. Tuân thủ quy định của pháp luật về bảo vệ an ninh mạng; kịp thời cung cấp thông tin liên quan đến an ninh mạng, nguy cơ đe dọa an ninh mạng và các hành vi xâm phạm khác, thực hiện yêu cầu và hướng dẫn của cơ quan quản lý nhà nước có thẩm quyền; giúp đỡ, tạo điều kiện cho người có trách nhiệm tiến hành các biện pháp bảo vệ an ninh mạng.

Mỗi người cần nghiên cứu và sử dụng tốt các biện pháp kỹ thuật bảo đảm an toàn thông tin như bảo vệ tài khoản cá nhân bằng xác thực mật khẩu đa lớp; tạo thói quen quét virus trước khi mở file; thực hiện sao lưu dự phòng trên ổ cứng ngoài, mạng nội bộ hoặc trên các dịch vụ lưu trữ đám mây (Google Drive, OneDrive); kiểm tra lộ lọt thông tin tài khoản cá nhân qua Trung tâm xử lý tấn công mạng Việt Nam.

Người dùng không nên vào những trang web lạ (hoặc trang web đen), những email chưa rõ danh tính và đường dẫn đáng nghi ngờ; cập nhật bản trình duyệt, hệ điều hành và các chương trình sử dụng; dùng những phần mềm diệt virus uy tín và được cập nhật thường xuyên, không tắt chương trình diệt virus trong mọi thời điểm. Khi phát hiện bị tấn công trên không gian mạng, nhanh chóng ngắt kết nối mạng; sử dụng các công cụ giải mã độc; báo cho người có trách nhiệm qua đường dây nóng.

2.5. Thứ năm: Phát huy vai trò, trách nhiệm của các cơ quan chuyên trách an ninh mạng, lãnh đạo, quản lý các địa phương, cơ quan, đơn vị, doanh nghiệp, nhà trường trong giáo dục nâng cao ý thức làm chủ và bảo vệ không gian mạng.

Các cơ quan chuyên trách an ninh mạng (Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao, Bộ Công an; Bộ Tư lệnh Tác chiến không gian mạng, Bộ Quốc phòng; lực lượng bảo vệ an ninh mạng tại bộ,

ngành, ủy ban nhân dân tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia) cung cấp đầy đủ thông tin về xu hướng phát triển, các nguy cơ từ không gian mạng; các biện pháp phòng, chống tấn công trên không gian mạng.

Các doanh nghiệp cung cấp dịch vụ trên không gian mạng tăng cường cảnh báo khả năng mất an ninh mạng do đơn vị mình cung cấp và hướng dẫn biện pháp phòng ngừa; xây dựng các phương án xử lý với sự cố an ninh mạng; phối hợp, tạo điều kiện cho lực lượng chuyên trách trong hoạt động bảo vệ an ninh mạng. Các cơ sở giáo dục sớm đưa nội dung giáo dục bảo đảm an ninh không gian mạng quốc gia vào chương trình dạy học phù hợp với ngành học, cấp học.

Lãnh đạo, quản lý các địa phương, cơ quan, đơn vị, doanh nghiệp, nhà trường cần nắm vững mọi hoạt động và tình hình tư tưởng cán bộ, đảng viên, quần chúng, có nội dung giáo dục, định hướng, điều chỉnh nhận thức đúng đắn, kịp thời; có trách nhiệm trong quản lý thông tin có liên quan tới cán bộ, đảng viên và quần chúng, có kế hoạch bảo vệ chính trị nội bộ trên không gian mạng.