

## I. NHẬN THỨC VỀ AN TOÀN THÔNG TIN TRÊN KHÔNG GIAN MẠNG

### 1. Khái niệm an toàn thông tin trên không gian mạng

#### a) An toàn thông tin mạng

- 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”***.

- Theo Nghị định Số: 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về Quản lý, cung cấp, sử dụng dịch vụ internet và thông tin trên mạng:

Thông tin trên mạng là thông tin được lưu trữ, truyền đưa, thu thập và xử lý thông qua mạng

Hệ thống thông tin là tập hợp các thiết bị viễn thông, công nghệ thông tin bao gồm phần cứng, phần mềm và cơ sở dữ liệu phục vụ cho hoạt động lưu trữ, xử lý, truyền đưa, chia sẻ, trao đổi, cung cấp và sử dụng thông tin.

“An toàn thông tin là sự bảo vệ thông tin và các hệ thống thông tin 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”.

- 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”***.

#### b) An ninh mạng

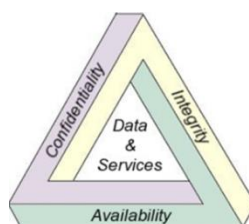
Ngày 12/6/2018, Luật An ninh mạng được Quốc hội khóa XIV thông qua quy định những nội dung cơ bản về bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia; phòng ngừa, xử lý hành vi xâm phạm an ninh mạng; triển khai hoạt động bảo vệ an ninh mạng và quy định trách nhiệm của cơ 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 việc 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.

Khái niệm “*Tội phạm sử dụng công nghệ cao*”, 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”.

Điểm chung trong nội hàm của các khái niệm về tội phạm công nghệ cao 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.



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 trên không gian mạng**

### **a) 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.

### **b) 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.

Các cơ quan đặc biệt nước ngoài, các thế lực thù địch, phản động tăng cường hoạt động tình báo, gián điệp, khủng bố, phá hoại hệ thống thông tin; tán phát thông tin xấu, độc hại nhằm tác động chính trị nội bộ, can thiệp, hướng lái chính sách, pháp luật của Việt Nam. Gia tăng hoạt động tấn công mạng nhằm vào hệ thống thông tin quan trọng quốc gia, hệ thống thông tin quan trọng về an ninh quốc gia. Theo thống kê, trung bình mỗi năm, qua kiểm tra, kiểm soát các cơ quan chức năng đã phát hiện trên 850.000 tài liệu chiến tranh tâm lý, phản động, ân xá quốc tế, tài liệu tuyên truyền tà đạo trái phép; gần 750.000 tài liệu tuyên truyền chống Đảng, Nhà nước được tán phát vào Việt Nam qua đường bưu chính. Từ 2010 đến 2019 đã có 53.744 lượt cổng thông tin, trang tin điện tử có tên miền .vn bị tấn công, trong đó có 2.393 lượt cổng thông tin, trang tin điện tử của các cơ quan Đảng, Nhà nước “.gov.vn”, xuất hiện nhiều cuộc tấn công mang màu sắc chính trị, gây ra những hậu quả nghiêm trọng.

Tội phạm và vi phạm pháp luật trong lĩnh vực thông tin diễn biến phức tạp, gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về nhiều mặt. Các hành vi phá hoại cơ sở hạ tầng thông tin; gây mất an toàn, hoạt động bình thường, vững mạnh của mạng máy tính, mạng viễn thông, phương tiện điện tử của các cơ quan, tổ chức, cá nhân và hệ thống thông tin vô tuyến điện,... đã và đang gây ra những thiệt hại lớn về kinh tế, xâm hại trực tiếp đến quyền, lợi ích hợp pháp của các cơ quan, tổ chức và cá nhân. Theo kết quả đánh giá an ninh mạng do Tập đoàn công nghệ Bkav thực hiện, trong năm 2019, chỉ tính riêng thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam đã lên tới 20.892 tỷ đồng (tương đương 902 triệu USD), hơn 1,8 triệu máy tính bị mất dữ liệu do sự lan tràn của các loại mã độc mã hóa dữ liệu tống tiền (ransomware), trong đó có nhiều máy chủ chứa dữ liệu của các cơ quan, gây đình trệ hoạt động của nhiều cơ quan, doanh nghiệp.

Hệ thống thông tin của Việt Nam còn tồn tại nhiều điểm yếu, lỗ hổng bảo mật dễ bị khai thác, tấn công, xâm nhập; tình trạng lộ, mất bí mật nhà nước qua hệ thống thông tin gia tăng đột biến; hiện tượng khai thác, sử dụng trái phép cơ sở dữ liệu, tài nguyên thông tin quốc gia, dữ liệu cá nhân người dùng diễn biến phức tạp; xuất hiện nhiều dịch vụ mới, hiện đại gây khó khăn cho công tác quản lý, kiểm soát của các cơ quan chức năng. Từ 2001 đến 2019, các cơ quan chức năng đã phát hiện hơn 1.100 vụ lộ, mất bí mật nhà nước, trong đó lộ, mất bí mật nhà nước qua hệ thống thông tin chiếm tỷ lệ lớn với trên 80% số vụ [1]. Tháng

3/2018, Facebook cũng đã để lộ dữ liệu cá nhân để một nhà phát triển bán lại cho Công ty Cambridge Analytica, dẫn tới 87 triệu dữ liệu thông tin người dùng bị lộ, trong đó có 427.466 tài khoản của người dùng Việt Nam

## **II. PHÒNG, CHỐNG VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG**

### **1. Các hành vi vi phạm pháp luật trên không gian mạng**

#### **a) Tin rác, tin giả**

- Tin rác Spam (viết tắt của Stupid Pointless Annoying Messages), 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.

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.

- 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 nẫu" 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:

+ Tin giả được lợi dụng vào các âm mưu chính trị và làm rối loạn xã hội.

+ 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 dễ 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.

b) 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:

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

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

+ 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;

+ 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 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;

+ 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;

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

- 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.

- 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.

- 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.

- 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.

- 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:

- + Tuyên truyền xuyên tạc, phỉ báng chính quyền nhân dân;
- + 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;
- + 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:

- + 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;
- + 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.

### c) 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, 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 suất 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, matkhu, 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.

#### d) 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.



#### e) Dark web

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.

### **2. Cơ sở pháp lý phòng, chống vi phạm pháp luật trên không gian mạng**

#### a) Bộ luật Hình sự năm 2015

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. Luật 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 đất nước.

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.

Bố cục của Bộ luật Hình sự gồm 26 Chương và 426 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 hình 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.

#### b) Luật An toàn thông tin mạng 2015

Mạng Internet đã và đang trở thành công cụ trọng 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.

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

Bố cục của Luật An toàn thông tin mạng gồm 08 Chương và 54 Điều:

- 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.

### c) Luật An ninh mạng 2018

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.

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

Bố cục của Luật An ninh mạng gồm 07 Chương, 43 Điều:

- 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; củng cố 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**

a) 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.

b) 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 truyền 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.

c) 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 găm 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...

d) Nâng cao ý thức phòng tránh, tự vệ và sử dụng 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 dữ liệu 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.

e) 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.

## **KẾT LUẬN**

Bài học đã đề cập đến vấn đề an toàn thông tin mạng, an ninh mạng và thực trạng đang ở mức báo động về các vụ lừa đảo qua mạng, đánh cắp thông tin và dữ liệu nhạy cảm, xâm nhập máy tính, hệ thống thông tin bất hợp pháp, xuất hiện nhiều phần mềm gián điệp, tin giả, tin rác... Để đối phó với tình hình an toàn thông tin ở mức báo động như hiện nay nước ta cần phải tập trung đào tạo nguồn nhân lực chất lượng cao và có đạo đức nghề nghiệp về an toàn thông tin. Với các bạn sinh viên, tầng lớp trí thức về công nghệ thông tin cần phải nhận thức rõ: An ninh thông tin là nội dung trọng tâm của an ninh quốc gia trong điều kiện mới, có mối quan hệ chặt chẽ với các vấn đề an ninh truyền thống khác như an ninh chính trị nội bộ, an ninh quân sự, an ninh văn hóa tư tưởng, an ninh kinh tế, an ninh xã hội... Nguy cơ gây mất an ninh thông tin là mối đe dọa lớn và ngày càng gia tăng đối với an ninh quốc gia, an ninh quốc tế. Qua đây thấy được vai trò quan trọng của mình trong việc phòng chống các hành vi vi phạm pháp luật trên không gian mạng nói riêng và trong bảo đảm an toàn thông tin mạng, an ninh mạng, trong giữ gìn an ninh quốc gia, trật tự an toàn xã hội nói chung.

## **I. TÀI LIỆU THAM KHẢO**

- [1]. Bộ luật Hình sự, Quốc hội Nước Cộng hòa xã hội chủ nghĩa Việt Nam, 2015.
- [2]. Luật An toàn thông tin mạng, Quốc hội Nước Cộng hòa xã hội chủ nghĩa Việt Nam, 2015.
- [3]. Luật An ninh mạng, Quốc hội Nước Cộng hòa xã hội chủ nghĩa Việt Nam, 2018.
- [4]. Nghị định số 72/2013/NĐ-CP ngày 15/7/2013 của Chính phủ về Quản lý, ban hành cung cấp, sử dụng dịch vụ internet và thông tin trên mạng
- [5]. Thông tư số 09/2014/TT-BTTTT ngày 19/ 08/ 2014 về Quy định chi tiết về hoạt động quản lý, cung cấp, sử dụng thông tin trên trang thông tin điện tử và mạng xã hội.
- [6]. Tài liệu tập huấn 2020, Bộ Giáo dục và Đào tạo, Vụ Giáo dục Quốc phòng và An ninh, 2020