Chuyên đề 2:

AN TOÀN THÔNG TIN VÀ CÁC HÀNH VI VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG TRONG HỌC SINH, SINH VIÊN. TÌNH HÌNH AN NINH CHÍNH TRỊ, TRẬT TỰ AN TOÀN XÃ HỘI TRONG NƯỚC LIÊN QUAN ĐẾN PHÒNG CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO VÀ TỆ NẠN XÃ HỘI.

Trung tá.TS Trịnh Trung Hiếu, Phó trưởng Khoa
Khoa An ninh mạng và phòng chống tội phạm sử dụng công nghệ cao
Học viện An ninh nhân dân

I. AN TOÀN THÔNG TIN VÀ CÁC HÀNH VI VI PHẠM PHÁP LUẬT TRÊN KHÔNG GIAN MẠNG TRONG HỌC SINH, SINH VIÊN

1. An toàn thông tin mạng

- *Thông tin mạng* là những thông tin được lưu trữ, truyền đưa, thu thập và xử lý thông qua mạng. Thông tin mạng bao gồm:

+ Thông tin công cộng: là thông tin trên mạng của một tổ chức, cá nhân được công khai cho tất cả các đối tượng mà không cần xác định danh tính, địa chỉ cụ thể của các đối tượng đó.

+ Thông tin riêng: là thông tin trên mạng của một tổ chức, cá nhân mà tổ chức, cá nhân đó không công khai hoặc chỉ công khai cho một hoặc một nhóm đối tượng đã được xác định danh tính, địa chỉ cụ thể.

+ Thông tin cá nhân: là thông tin trên mạng được xác định gắn với việc xác định danh tính một người cụ thể.

+ Thông tin bí mật nhà nước: là thông tin ở mức Mật, Tối mật, Tuyệt mật theo quy định của pháp luật về bảo vệ bí mật nhà nước.

- *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 đảm bảo tính nguyên vẹn, tính bảo mật và tính khả dụng của thông tin *(*Điều 3, Luật An toàn thông tin mạng 2015).

Một thông tin, hệ thống thông tin được xem là an toàn khi đảm bảo các thuộc tính cơ bản: tính bí mật, tính toàn vẹn, tính sẵn sàng. Ngoài ra còn có các thuộc tính khác như tính không thể chối cãi, tính xác thực.

+ Tính bí mật: tránh lộ thông tin đến những đối tượng không được xác thực hoặc để lọt thông tin vào các hệ thống khác. Đảm bảo tính bí mật của thông tin tức là thông tin chỉ được truy cập (đọc) bởi những đối tượng (người, chương trình máy tính) được cấp phép.

+ Tính toàn vẹn: dữ liệu không thể bị chỉnh sửa mà không bị phát hiện. Đảm bảo tính toàn vẹn thông tin tức là thông tin chỉ được phép xóa hoặc sửa bởi những đối tượng được cho phép và phải đảm bảo thông tin vẫn còn chính xác khi được lưu trữ hay truyền đi.

+ Tính sẵn sàng: mọi hệ thống thông tin đều phục vụ mục đích riêng của nó và thông tin phải luôn sẵn sàng khi cần thiết. Đảm bảo độ sẵn sàng của thông tin, thức là thông tin có thể được truy xuất bởi những người được phép vào bất kỳ khi nào họ muốn.

Tính xác thực: Trong hoạt động tính toán, kinh doanh qua mạng và an toàn thông tin, tính xác thực là vô cùng cần thiết để đảm bảo rằng dữ liệu, giao dịch, kết nối hoặc các tài liệu (tài liệu điện tử hoặc tài liệu cứng) đều là thật. Nó cũng quan trọng cho việc xác nhận rằng các bên liên quan biết họ là ai trong hệ thống.

Tính không thể chối cãi: không thể chối cãi có nghĩa rằng một bên giao dịch không thể phủ nhận việc họ đã thực hiện giao dịch với bên khác. Điển hình như trong khi giao dịch mua hàng qua mạng, khi khách hàng đã gửi số thẻ tín dụng cho bên bán, đã thanh toán thành công thì bên bán không thể phủ nhận việc họ đã nhận được tiền (trừ trường hợp hệ thống không đảm bảo tính an toàn thông tin trong khi giao dịch).

- Yếu tố tác động đến an toàn thông tin mạng

Yếu tố khách quan, bao gồm: Ý đồ, chính sách, chiến lược của các nước đối với Việt Nam và chính sách an ninh, an toàn thông tin của các quốc gia; đấu tranh giành chủ quyền quốc gia trên không gian mạng, cạnh tranh trong phát triển công nghệ thông tin, giành và giữ tài nguyên thông tin,... có tác động cả tích cực và tiêu cực đối với an ninh, an toàn thông tin mạng Việt Nam. Xu thế toàn cầu hóa, hội nhập quốc tế và sự phát triển của các cuộc cách mạng công nghiệp, cách mạng thông tin vừa tạo ra thời cơ, vừa đưa đến những thách thức to lớn đối với an ninh, an toàn thông tin của Việt Nam. Lợi ích cùng sự bành trướng của các tập đoàn công nghệ thông tin, truyền thông và sự liên hệ, chịu sự chi phối của nó từ các tổ chức quân sự, tình báo, phản gián các nước; hoạt động của các thế lực thù địch sử dụng hệ thống thông tin xâm phạm an ninh quốc gia, tấn công, phá hoại cơ sở hạ tầng và an ninh thông tin, tiến hành chiến tranh thông tin đối với Việt Nam; hoạt động của tội phạm, hacker và các nhóm tin tặc nước ngoài; các sự cố, tình huống nguy hiểm về an ninh thông tin;… là những yếu tố tác động tiêu cực, xâm hại đến an ninh thông tin, độc lập, chủ quyền, lợi ích quốc gia trên không gian mạng.

Yếu tố chủ quan, bao gồm: Tổ chức, phối hợp lực lượng, hợp tác trong bảo đảm an ninh, an toàn thông tin; Đường lối, chính sách, pháp luật về bảo đảm an ninh thông tin của Đảng, Nhà nước; Nguồn nhân lực bảo đảm an ninh thông tin, năng lực tự chủ, tự bảo vệ của các tổ chức, cá nhân khi tham gia hoạt động thông tin; Trình độ công nghệ (cả phần cứng và phần mềm), năng lực tự chủ về công nghệ, khả năng ứng phó, phục hồi trước các hoạt động tấn công nhằm vào hệ thống thông tin của Việt Nam; Nguồn lực thông tin, tài nguyên thông tin và các hệ cơ sở dữ liệu quốc gia; Hiệu lực, hiệu quả quản lý nhà nước về an ninh, an toàn thông tin; Ý thức người dùng về các nguy cơ gây mất an ninh, an toàn thông tin;

Sự suy thoái tư tưởng chính trị, đạo đức lối sống, "tự diễn biến", "tự chuyển hóa" trong nội bộ, nhất là trong các cơ quan, tổ chức quản lý và hoạt động thông tin. Những yếu tố trên nếu được bảo đảm sẽ có tác động tích cực, góp phần tăng cường, bảo đảm an ninh, an toàn thông tin của Việt Nam; ngược lại, sẽ tạo nguy cơ, tình huống gây mất an ninh, đe dọa gây mất an ninh, an toàn thông tin ở các cấp độ khác nhau.

Các yếu tố tác động đến an toàn thông tin cả khách quan và chủ quan, cả bên trong và bên ngoài đều rất quan trọng và luôn có mối quan hệ chặt chẽ, có sự chuyển hóa lẫn nhau. Trong đó, các yếu tố chủ quan, nhất là, nguồn nhân lực bảo đảm an ninh, an toàn thông tin, năng lực tự chủ, tự bảo vệ của các tổ chức, cá nhân khi tham gia hoạt động thông tin, ý thức người dân, trình độ công nghệ (cả phần cứng và phần mềm), năng lực tự chủ về công nghệ, khả năng ứng phó, phục hồi trước các hoạt động tấn công nhằm vào hệ thống thông tin của Việt Nam là yếu tố quyết định. Âm mưu, hoạt động của các thế lực thù địch, tội phạm sử dụng hệ thống xâm phạm an ninh quốc gia, trật tự an toàn xã hội, tấn công, phá hoại cơ sở hạ tầng và an ninh, an toàn thông tin, tiến hành chiến tranh thông tin đối với Việt Nam có tính chất đặc biệt nguy hiểm; có thể dẫn đến mất kiểm soát an ninh thông tin, vô hiệu hóa khả năng lãnh đạo, điều hành, quản lý của nhà nước trong bối cảnh cách mạng công nghiệp lần thứ tư hiện nay. Một số nhóm tin tặc nước ngoài bị các thế lực thù địch, chính phủ một số nước lợi dụng vào các hoạt động tấn công mạng, chiếm quyền điều khiển hệ thống thông tin quan trọng về an ninh quốc gia nhằm mục đích chính trị hoặc kinh tế (đòi trả tiền chuộc, gây sức ép về kinh tế); từ vấn đề tội phạm hình sự dễ chuyển hóa thành các vấn đề chính trị, đối ngoại là yếu tố nguy hiểm thường xuyên đe dọa gây mất an ninh, an toàn thông tin.

2. Các hành vi vi phạm pháp luật phổ biến trên không gian mạng trong học sinh, sinh viên.

- Đăng tải, chia sẻ, tán phát các thông tin tuyên truyền chống nhà nước Cộng hòa XHCN Việt Nam. Hành vi phổ biến là thiết lập các website, blog, trang fanpage, kênh You Tube,… để đăng tải, chia sẻ các bài viết, hình ảnh, video clip có nội dung 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,…

Điển hình như trường hợp Phan Kim Khánh, sinh viên Khoa Quốc tế, Đại học Thái Nguyên. Năm 2015, Khánh đã lập và quản trị 02 blog lấy tên là "Báo tham nhũng" và "Tuần Việt Nam", 03 trang trên mạng xã hội Facebook lấy tên là "Báo tham nhũng", "Tuần báo Việt Nam" và "Dân chủ TV"; 02 kênh trên mạng xã hội You Tube lấy tên là "Việt Báo TV" và "Việt Nam online" liên tục đăng nhiều thông tin có nội dung bịa đặt, xuyên tạc nhằm chống Nhà nước Cộng hòa xã hội chủ nghĩa Việt Nam, phần lớn được lấy từ các trang mạng phản động khác.

Ngày 21/3/2017, Phan Kim Khánh bị cơ quan An ninh điều tra Công an tỉnh Thái Nguyên bắt giữ về tội "Tuyên truyền chống nhà nước CHXHCN Việt Nam"; ngày 25/10/2017, Tòa án nhân dân tỉnh Thái Nguyên đã xét xử, tuyên phạt Khánh 6 năm tù giam về tội danh trên.

- Tham gia, sử dụng không gian mạng nhất là mạng xã hội kích động biểu tình, bạo loạn, phá rối an ninh. Hành vi phổ biến là tham gia các hội, nhóm trên không gian mạng thường xuyên đăng tải, chia sẻ thông tin kích động các hoạt động xâm phạm ANQG, trật tự an toàn xã hội; tham gia các phong trào chống đối trên mạng (như đồng loạt thay đổi avatar để phản đối một chủ trương, chính sách của Đảng, Nhà nước, địa phương); tham gia, hưởng ứng việc sử dụng không gian mạng để kích động biểu tình (như biểu tình phản đối luật An ninh mạng, Luật về đơn vị hành chính - kinh tế đặc biệt,…); sử dụng mạng xã hội để kích động, lôi kéo người khác biểu tình; từ việc nghe theo hoạt động kích động trên mạng mà tham gia biểu tình, tụ tập đông người, khiếu kiện trái quy định của pháp luật trên thực tế.

Theo Thông tư số 10/2016/TT-BGDĐT ngày 05/4/2016 của Bộ Giáo dục và Đào tạo Ban hành quy chế công tác sinh viên đối với chương trình đào tạo hệ đại học chính quy, phần phụ lục về nột số nội dung vi phạm và khung xử lý kỷ luật sinh viên có quy định: (1) Sinh viên kích động, lôi kéo người khác biểu tình: lần 1 bị đình chỉ có thời hạn; lần 2 bị buộc thôi học; nếu hành vi ở mức độ nghiêm trọng thì giao cho cơ quan chức năng xử lý theo quy định của pháp luật. (2) Sinh viên tham gia biểu tình, tụ tập đông người, khiếu kiện trái quy định của pháp luật thì các mức xử lý là: vi phạm lần 1 bị xử phạt khiển trách; vi phạm lần 2 bị xử phạt cảnh cáo; vi phạm lần 3 bị xử phạt đình chỉ có thời hạn; vi phạm lần 4 bị buộc thôi học. Nếu hành vi tham gia ở mức độ nghiêm trọng thì giao cho cơ quan chức năng xử lý theo quy định của pháp luật.

- Tham gia các tổ chức phản động, khủng bố, các đợt tuyển lựa, đào tạo, huấn luyện trên không gian mạng của các tổ chức phản động, khủng bố: tham gia các diễn đàn trên không gian mạng của các tổ chức khủng bố như "Việt Tân", "Chính phủ quốc gia Việt Nam lâm thời", "Triều đại Việt"; nhận tài trợ của các tổ chức khủng bố; tham gia các khóa đào tạo, huấn luyện trực tuyến về phương thức, hoạt động khủng bố phá hoại; các video hướng dẫn cách chế tạo bom xăng để phục vụ hoạt động khủng bố, phá hoại, ám sát,… Trong năm 2021, Bộ Công an đã cảnh báo về việc các tổ chức khủng bố nhất là "Việt Tân" tăng cường móc nối, lôi kéo học sinh, sinh viên đặc biệt là du học sinh Việt Nam ở nước ngoài tham gia các hoạt động biểu tình chống Nhà nước, tham gia hội họp, huấn luyện của Việt Tân để từ đó tuyển lựa thành viên, chỉ đạo xâm nhập về nước hoạt động. Nổi bật là trường hợp N.T.H.T ở thành phố Uông Bí, trong thời gian du học tại Nhật Bản đã bị số cốt cán của tổ chức Việt Tân lợi dụng việc hỗ trợ du học sinh Việt Nam ở nước ngoài trong học tập, tìm kiếm việc làm sau đó lôi kéo tham gia

các hoạt động biểu tình chống đối, tham gia các buổi hội họp xuyên tạc về tình hình nhân quyền tại Việt Nam, vu cáo Việt Nam đàn áp nhân quyền.

Các tổ chức khủng bố, điển hình như tổ chức "Triều đại Việt" triệt để sử dụng các tiện ích trên không gian mạng đặc biệt là Youtube, Facebook đăng tải các video clip có nội dung tuyên truyền về tổ chức, xuyên tạc chủ trương, đường lối của Đảng, chính sách, pháp luật của Nhà nước, kích động người dân xuống đường biểu tình, bạo loạn; từng bước tiếp cận, tác động đối tượng trong nước có nhận thức mơ hồ về chính trị, cần kíp về tài chính, nhất là trong học sinh, sinh viên để lôi kéo tham gia, tiến hành các hoạt động khủng bố, phá hoại theo chỉ đạo của tổ chức. Năm 2018, đối tượng Trương Nguyễn Minh Trí, thành viên tổ chức Chính phủ Việt Nam lâm thời đã nhận chỉ thị của các đối tượng bên ngoài, trực tiếp tiếp xúc, xúi giục, lôi kéo các em học sinh lớp 9 và lớp 10 tại Bình Tân tham gia đi biểu tình, làm đơn xin gia nhập tổ chức Chính phủ Việt Nam lâm thời, qua đó tiến hành bạo động,… Hay trường hợp của Nguyễn Phương Uyên, sinh viên trường Đại học Công nghiệp thực phẩm thành phố Hồ Chí Minh, là 1 đoàn viên tiêu biểu; tháng 4 năm 2012, Uyên quen Nguyễn Thiện Thành qua mạng xã hội facebook, từ đó tham gia tổ chức "Tuổi trẻ yêu nước" – 1 tổ chức phản động ở nước ngoài được thành lập với âm mưu lật đổ chính quyền. Ngày 10/10/2012, Uyên tiến hành rải truyền đơn trên cầu vượt An Sương (xã Bà Điểm, huyện Hóc Môn, thành phố Hồ Chí Minh) sau đó bị cơ quan Công an phát hiện, xử lý hình sự về Tội tuyên truyền chống Nhà nước Cộng hòa XHCN Việt Nam.

- Tấn công mạng nhằm vào hệ thống thông tin của các cơ quan, tổ chức ở trung ương và địa phương. Điển hình như vụ việc năm 2017, Cục An ninh mạng Bộ Công an đã xác minh, phát hiện L.C.K.D (sinh năm 2002, trú tại Phường 15, quận Tân Bình, Thành phố Hồ Chí Minh) đã khai thác lỗ hổng bảo mật, tấn công website của sân bay Tân Sơn Nhất; phát hiện P.H.H (sinh năm 2002, trú tại huyện Trảng Bom, tỉnh Đồng Nai) đã tấn công, thay đổi giao diện, để lại thông báo trên website của các sân bay Đà Nẵng, Phú Quốc, Rạch Giá, Tuy Hòa. Hai học sinh lớp 9 với mục đích khám phá, mong muốn khoe thành tích trong giới hacker đã tấn công hàng loạt các cảng hàng không ở Việt Nam, tiềm ẩn nguy cơ gây ra những hậu quả nghiêm trọng về an ninh, trật tự.

Hay trong năm 2022, Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao đã phát hiện T.G.K 16 tuổi tại Hà Tĩnh đã tiến hành tấn công từ chối dịch vụ vào Cổng thông tin của Chính phủ; của Bộ Quốc phòng, Trường Đại học Hà Tĩnh; tấn công thay đổi giao diện của nhiều website ở Việt Nam. Tiến hành kiểm tra máy tính để bàn và khai thác các tài khoản trên mạng (facebook, email, youtube,…), lực lượng Công an thu được nhiều công cụ sử dụng để tấn công mạng, tấn công từ chối dịch vụ, 128 trang tài liệu, 01 đĩa CD lưu lại các hình ảnh, video liên quan đến hoạt động vi phạm pháp luật của học sinh này.

- Đăng tải, tán phát thông tin giả, thông tin sai sự thật trên Internet, mạng xã hội. Sử dụng mạng xã hội để đăng tải, chia sẻ thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác; thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán; thông tin trên không gian mạng có nội dung bịa đặt, 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,…

Điển hình như trường hợp của Nguyễn Lê Tấn Tài, sinh năm 2004, quê Đồng Nai, sinh viên năm thứ nhất của Trường Đại học Kinh tế Thành phố Hồ Chí Minh, admin fanpage UEH Confessions đã đăng tải bài viết có nội dung sai sự thật chuyện nữ sinh Trường Đại học Ngoại ngữ - Tin học thành phố Hồ Chí Minh (HUFLIT) đang học giáo dục quốc phòng an ninh tại Trường Quân sự Quân khu 7 nhảy lầu tự tử do bị xâm hại". Ngày 26/7/2023, Tòa án Quân sự Quân khu 7 đã mở phiên tòa xét xử, tuyên phạt Nguyễn Lê Tấn Tài 12 tháng cải tạo không giam giữ về tội "Đưa trái phép thông tin mạng máy tính".

- Sử dụng không gian mạng để thực hiện hành vi lừa đảo chiếm đoạt tài sản: Trực tiếp sử dụng mạng để thực hiện hành vi lừa đảo chiếm đoạt tài sản hoặc tham gia các đường dây lừa đảo chiếm đoạt tài sản xuyên quốc gia (được thuê để điều hành hệ thống, chọn kịch bản lừa đảo để tiến hành lừa các nạn nhân; được các đối tượng thuê mở tài khoản ngân hàng, đăng ký thông tin thuê bao phục vụ hoạt động lừa đảo,…). Trên thực tế, các đối tượng lừa đảo thường cung cấp cho học sinh, sinh viên điện thoại sẵn sim để đăng ký mở tài khoản thanh toán và dịch vụ Internet banking, sms banking sau đó yêu cầu học sinh, sinh viên trả lại điện thoại, cung cấp thông tin, mật khẩu xác thực (OTP); các đối tượng cũng thu thập dữ liệu sinh trắc học (khuôn mặt) của học sinh, sinh viên (Face ID) để phục vụ xác minh danh tính của khách hàng khi có yêu cầu. Các tài khoản này sau đó được sử dụng vào mục đích vi phạm pháp luật như rửa tiền, trốn thuế, lừa đảo chiếm đoạt tài sản, tài trợ khủng bố,…

Độ tuổi thực hiện hành vi sử dụng không gian mạng để lừa đảo chiếm đoạt tài sản ngày càng trẻ hóa, phát hiện nhiều học sinh, sinh viên thực hiện tội phạm này. Điển hình như năm 2023, nhóm sinh viên gồm 08 đối tượng Dương Ngô Tùng (SN 2002), Nguyễn Thị Hằng (SN 2002), Nguyễn Thế Minh (SN 2004), Nguyễn Hữu Phong (SN 2002), Hoàng Văn Trung (SN 2002), Bùi Ngọc Duy (SN 2002), Hoàng Thị Minh Dương (SN 2004) cùng trú tại Bắc Giang và Trần Đình Nam (SN 2004) trú tại Lào Cai đã sử dụng tài khoản facebook, zalo xưng danh "Thầy Thế" đăng bài viết có khả năng làm lễ giải hạn, cầu tài lộc, tư vấn mua lá

bùa cầu tài lộc, dâng sao giải hạn,… để tiếp cận nạn nhân rồi yêu cầu chuyển khoản làm lễ. Với thủ đoạn trên, từ tháng 5 đến tháng 6/2023, nhóm đối tượng này đã lừa đảo, chiếm đoạt hơn 2,5 tỷ đồng của nhiều nạn nhân.

Hay trường hợp đối tượng Võ Đình Tuấn, sinh viên năm 2, Trường Đại học Kiến trúc Đã Nẵng đã chiếm đoạt Facebook, email của nhiều Việt kiều có bạn bè, người thân ở Việt Nam để lừa đảo. Giả danh Việt kiều, đối tượng trò chuyện với nạn nhân trong danh sách bạn bè, đề nghị mua thẻ cào điện thoại ở Việt Nam gửi mã qua, mỗi thẻ cào 100.000đ sẽ đổi được số tiền 15 - 20 USD ở nước ngoài (nước sở tại Việt kiều đang sống), tiền lời sẽ chia nhau. Với thủ đoạn trên, Tuấn đã chiếm đoạt tài sản của nhiều nạn nhân với số tiền hơn 800 triệu đồng.

- *Sử dụng không gian mạng để đánh bạc và tổ chức đánh bạc.* Nổi bật là các hành vi tham gia đánh bạc trên mạng dưới 02 hình thức phổ biến là tín chấp (đánh bạc trước, trả tiền sau) và thế chấp (đánh bạc trực tiếp trên trang web, thanh toán qua tài khoản ngân hàng).

Các hình thức đánh bạc tín chấp phổ biến là xóc đĩa trực tuyến, cá độ bóng đá trực tuyến, lô đề trực tuyến. Với hình thức này, học sinh, sinh viên không cần bỏ tiền ra trước; dễ tham gia, thao tác đơn giản, khó kiểm soát được lượng tiền đánh bạc, hết tiền chỉ cần gọi điện là có. Khi thua bạc, học sinh, sinh viên nào không có tiền thanh toán sẽ bị ép trả tiền theo kiểu xã hội đen như giữ người trái pháp luật, buộc gán nhà cửa, tài sản,...

Các hình thức đánh bạc thế chấp phổ biến là cá cược thể thao (bóng đá, tennis, cầu lông, bóng rổ, golf, đua ngựa,…); casino trực tuyến, keno sổ xố, pocker. Đánh bạc theo hình thức này, học sinh, sinh viên phải lập 2 tài khoản (tài khoản đánh bạc + tài khoản ngân hàng), phải ứng trước tiền qua tài khoản ngân hàng. Nhà cái ở nước ngoài, đăng ký kinh doanh và đặt máy chủ ở các nước mà đánh bài là hợp pháp.

Thời gian qua, lực lượng Công an phát hiện, xử lý nhiều đường dây đánh bạc, tổ chức đánh bạc qua mạng, thu hút nhiều người tham gia trong đó có cả học sinh, sinh viên. Điển hình như cuối năm 2022, Phòng PA05 Công an tỉnh Bắc Giang đã phát hiện đối tượng Ngô Đức Hạ (Việt Yên, Bắc Giang) thông qua Trần Đỗ Đức Nghĩa - sinh viên Đại học, giỏi về công nghệ thông tin lập trình website để tổ chức đánh bạc dựa trên mã giao dịch của tài khoản ví điện tử Momo. Các đối tượng đã nghiên cứu, lập trình, quản trị điều hành website "clmm.me" và "clmmz.me", thuê địa chỉ IP, máy chủ đặt tại Mỹ để tổ chức đánh bạc. Đến khi bị phát hiện, xử lý, tổng số tiền giao dịch đánh bạc khoảng 2.800 tỷ đồng. Trong số các con bạc tham gia, có nhiều người là sinh viên các trường đại học lớn như Bách khoa Hà Nội, FPT Hà Nội, Đại học Quốc gia Hà Nội, Đại học Khoa học và Công nghệ Hà Nội,…

- Thực hiện các tội phạm khác trong lĩnh vực công nghệ thông tin, mạng viễn thông: sản xuất, mua bán, trao đổi hoặc cho tặng công cụ, thiết bị, phần mềm

để sử dụng vào mục đích trái pháp luật; tán phát chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; cản trở hoặc gây rối loạn hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; đưa hoặc sử dụng trái phép thông tin mạng máy tính, mạng viễn thông; xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác; thu thập, tàng trữ, trao đổi, mua bán, công khai hóa trái phép thông tin về tài khoản ngân hàng.

Điển hình như năm 2019, cơ quan Công an đã bắt giữ nhóm 04 đối tượng là sinh viên Trường Đại học Công nghệ thông tin Thái Nguyên và Đại học Công nghiệp Thái Nguyên. 4 sinh viên này đã dùng công cụ rà quét lỗ hổng các website của 04 công ty trung gian thanh toán để thực hiện hành vi xâm nhập trái phép, chiếm đoạt dữ liệu, tạo khống số dư cho những tài khoản là ví điện tử, sau đó sử dụng những tài khoản này để mua thẻ cào rồi bán lại và chuyển tiền về các tài khoản ngân hàng thu lợi bất chính hơn 3,2 tỷ đồng.

Tháng 4/2024, Công an thành phố Đà Nẵng phát hiện nhóm đối tượng gồm L.N.H.N (21 tuổi), P.Q.N.H (18 tuổi), M.N.C (19 tuổi) là sinh viên trên địa bàn thành phố Đà Nẵng đã phát tán hàng chục ngàn mã độc, chiếm tài khoản mạng xã hội của nhiều tổ chức, cá nhân, thu thập dữ liệu trong thiết bị điện tử của người dùng. Thủ đoạn của các đối tượng là sử dụng các tài khoản mạng xã hội Linkedin đăng các bài viết quảng cáo sản phẩm, tuyển dụng, kêu gọi đầu tư, gửi các tập tin có chứa đường dẫn tự động tải mã độc nhằm dẫn dụ người khác bấm vào xem nội dung, từ đó chiếm quyền sử dụng tài khoản Business manager trên Facebook của nạn nhân rồi sử dụng vào hoạt động vi phạm pháp luật nhằm thu lợi bất chính. Ngày 25/4/2024, Công an thành phố Đà Nẵng đã khởi tố vụ án hình sự "Xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác" để điều tra, làm rõ hành vi của các đối tượng.

- Các hành vi vi phạm pháp luật khác về trật tự an toàn xã hội: Sử dụng không gian mạng để mua bán trái phép văn bằng, chứng chỉ giả, mua bán ma túy, vũ khí, vật liệu nổ; mua bán, sử dụng trái phép dữ liệu cá nhân của người dùng; sử dụng không gian mạng để hoạt động mại dâm, tán phát văn hóa phẩm đồi trụy; vi phạm pháp luật trong hoạt động quảng cáo trực tuyến,…

Điển hình như vào tháng 1/2023, Cục Cảnh sát hình sự Bộ Công an đã phát hiện Hoàng Thị Nhật Lệ, sinh viên 1 Trường Đại học trên địa bàn thành phố Hà Nội thường xuyên sử dụng tài khoản zalo cá nhân "Hini Nguyễn và Luna" lập ra các hội nhóm để kết nối, trao đổi với người bán dâm và người mua dâm ở nhiều địa phương trong cả nước để môi giới mại dâm. Lệ và gái mại dâm không trực tiếp biết nhau mà chỉ tương tác qua mạng xã hội. Giá mua dâm dao động từ 10 triệu đến 15 triệu đồng/lượt; qua đêm hoặc sextour từ 1.000 đến 2.000 USD /lần tùy thuộc vào nhan sắc gái bán dâm. Ngày 8/1/2023, Cơ quan Cảnh sát điều tra

Công an thành phố Hà Nội đã ra lệnh bắt đối với Hoàng Thị Nhật Lệ về hành vi "Môi giới mại dâm".

II. TÌNH HÌNH AN NINH CHÍNH TRỊ, TRẬT TỰ AN TOÀN XÃ HỘI TRONG NƯỚC LIÊN QUAN ĐẾN PHÒNG, CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO VÀ TỆ NẠN XÃ HỘI

- Các thế lực thù địch, phản động tăng cường hoạt động gián điệp mạng; khủng bố mạng; triệt để sử dụng không gian mạng để tuyên truyền phá hoại tư tưởng, phản biện chính sách, hình thành các hội, nhóm,… nhằm tác động chính trị nội bộ, can thiệp, hướng lái chính sách, pháp luật an ninh thông tin của Việt Nam. Các đối tượng thiết lập hàng ngàn website, blog, triệt để lợi dụng mạng xã hội để tán phát các quan điểm sai trái, thù địch, kích động biểu tình, bạo loạn, phá rối an ninh; đào tạo, huấn luyện khủng bố,… Hoạt động tuyên truyền chống Đảng, Nhà nước của các thế lực thù địch đã tạo ra một khối lượng thông tin xấu, độc lớn trên không gian mạng, hàng ngày, hàng giờ tiêm nhiễm vào cộng đồng mạng Việt Nam, nhất là giới trẻ tiềm ẩn nhiều nguy cơ gây mất an ninh, trật tự.

- Gia tăng các hoạt động tấn công mạng trên diện rộng và đối với hệ thống thông tin quan trọng liên quan đến an ninh quốc gia, nhất là các cuộc tấn công nhằm vào cơ quan Chính phủ, hệ thống tài chính, ngân hàng, hàng không, website của cơ quan, tổ chức, tập đoàn kinh tế lớn tại Việt Nam. Thống kê cho thấy, giai đoạn 2010 - 2021 đã có 28.527 trang mạng tên miền ".vn" bị tấn công, trong đó có nhiều trang tên miền ".gov.vn" của các cơ quan nhà nước. Xuất hiện nhiều cuộc tấn công mang màu sắc chính trị, gây ra những hậu quả nghiêm trọng, làm rối loạn hoạt động lãnh đạo, điều hành, quản lý kinh tế, xã hội của cơ quan, tổ chức. Nhiều cơ quan, ban, ngành của Đảng, Nhà nước bị tin tặc nước ngoài xâm nhập, kiểm soát, tấn công, thay đổi cơ sở dữ liệu, thu thập bí mật nhà nước, gây mất an ninh, trật tự. Theo số liệu của Cục An toàn thông tin, trong năm 2022 có hơn 11.213 cuộc tấn công mạng hướng vào Việt Nam, trong đó có 3.930 cuộc tấn công giả mạo (phishing), 1.524 cuộc tấn công thay đổi nội dung (deface), 5.759 cuộc tấn công phần mềm độc hại (mailware). Theo tổng hợp của Cục An toàn thông tin, năm 2023 ghi nhận 13.900 vụ tấn công an ninh mạng vào các hệ thống tại Việt Nam. Các mục tiêu chịu nhiều cuộc tấn công nhất là các cơ quan Chính phủ, hệ thống ngân hàng, tổ chức tài chính, hệ thống công nghiệp và các hệ thống trọng yếu khác.

Trong những năm qua cũng phát hiện nhiều "chiến dịch" tấn công mạng có chủ đích nhằm vào Việt Nam do các nhóm tin tặc nước ngoài hoạt động theo sự chỉ đạo của các nhà nước, chính phủ nước ngoài tiến hành. Mục đích của chúng nhằm phá hoại hệ thống thông tin liên lạc, gây mất kiểm soát thông tin, làm rối loạn hoạt động lãnh đạo, điều hành, quản lý kinh tế, xã hội của cơ quan, tổ chức; hoặc răn đe, gây sức ép về chính trị đối với nước ta trước vụ việc phức tạp, có liên quan đến quan hệ ngoại giao giữa hai nước. Điển hình như vụ tin tặc nước ngoài tấn công hệ thống máy tính của Hãng hàng không Việt Nam Airlines và Hãng hàng không VietJet Air, chiếm quyền điều khiển, thay đổi giao diện, thay thế file âm thanh

gốc, chèn các nội dung xuyên tạc liên quan đến tình hình biển, đảo. Bên cạnh đó, nhiều hệ thống thông tin của các doanh nghiệp, tập đoàn lớn (như Công ty Viễn thông Quốc tế - đơn vị quản lý vệ tinh VINASAT 1, Tập đoàn Viễn thông Quân đội, Tập đoàn Dầu khí quốc gia Việt Nam), cơ quan, ban, ngành của Đảng, Nhà nước (các Văn phòng Trung ương, Bộ Tài chính, Bộ Ngoại giao) đều đã từng bị tin tặc nước ngoài xâm nhập, kiểm soát, tấn công, thay đổi cơ sở dữ liệu, thu thập bí mật nhà nước.

- Tội phạm và vi phạm pháp luật trên không gian mạng diễn biến phức tạp, gia tăng về số vụ, thủ đoạn tinh vi, gây thiệt hại nghiêm trọng về nhiều mặt. Nổi lên thời gian qua là việc sử dụng không gian mạng để lừa đảo chiếm đoạt tài sản; đánh bạc và tổ chức đánh bạc qua Internet; sử dụng không gian mạng để mua bán trái phép dữ liệu cá nhân người dùng, mua bán trái phép văn bằng, chứng chỉ giả, mua bán ma túy, vũ khí, vật liệu nổ; sử dụng không gian mạng để hoạt động mại dâm, tán phát văn hóa phẩm đồi trụy; hoạt động tín dụng đen qua mạng; phát tán virus, phần mềm độc hại gây thiệt hại cho người sử dụng,… Theo kết quả đánh giá an ninh mạng do Tập đoàn công nghệ Bkav thực hiện, trong năm 2023, riêng thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam ở mức 17.300 tỷ đồng (tương đương 716 triệu USD). BKAV cũng phát hiện hơn 15.000 phần mềm gián điệp trên điện thoại di động mà nổi bật nhất là vụ việc VN84App, phần mềm thu thập tin nhắn OTP giao dịch ngân hàng đã lây nhiễm vào hàng nghìn smartphone tại Việt Nam, thu thập dữ liệu cá nhân người dùng thực hiện các giao dịch bất hợp pháp, chiếm đoạt hàng trăm tỷ đồng của người sử dụng.

Các đối tượng hoạt động "tín dụng đen" trên mạng có xu hướng nhằm vào học sinh, sinh viên do đây là tầng lớp có tuổi đời còn trẻ, thiếu kinh nghiệm sống, chưa có kinh tế, phụ thuộc gần như tuyệt đối vào bố mẹ, có những học sinh, sinh viên chịu áp lực từ học phí, thuê nhà, khi phí sinh hoạt,… nên dễ rơi vào bẫy của các đối tượng hoạt động "tín dụng đen". Trở thành nạn nhân của "tín dụng đen" sẽ ảnh hưởng đến tinh thần, khả năng học tập của học sinh, sinh viên do phải đối mặt với áp lực trả nợ. Khi không có tiền trả nợ, các em hoặc phải xin tiền bố mẹ, hoặc phải tự tìm đến con đường dẫn tới hành vi phạm tội.

Hoạt động sử dụng mạng xã hội để "livestream" buôn bán các sản phẩm, hàng hóa nhập lậu, hàng không rõ nguồn gốc xuất xứ, hàng giả, hàng cấm diễn ra phổ biến; hoạt động quảng cáo trực tuyến diễn ra tràn lan trên các trang tin điện tử, mạng xã hội với nhiều nội dung vi phạm pháp luật như cờ bạc, mại dâm; công tác quản lý đăng ký, sử dụng tài khoản ví điện tử, giám sát, kiểm tra các giao dịch trực tuyến trong thương mại điện tử còn nhiều hạn chế, dễ bị các đối tượng lợi dụng vào hoạt động xâm hại an ninh, trật tự,…

- Sự bùng nổ của các thiết bị thông minh, trí tuệ nhân tạo (AI), nhất là ứng dụng trên smartphone. Đây là mối đe dọa trực tiếp đến an ninh mạng, đến trật tự an toàn xã hội do người dùng cung cấp quá nhiều quyền truy cập, cũng như cung

cấp thông tin cá nhân trên mạng xã hội, ứng dụng,… dẫn đến tình trạng bị chiếm đoạt, lợi dụng vi phạm pháp luật. Đặc biệt, mối đe dọa đến từ các thiết bị IoT đang là vấn đề lớn, hiện chưa có giải pháp tổng thể đảm bảo an toàn, an ninh mạng, bảo vệ bí mật nhà nước cho các thiết bị IoT, do đó, nhiều vụ lộ, lọt thông tin cá nhân nhạy cảm, riêng tư,… đã bị phát tán trên mạng. Mặc dù các cơ quan chức năng đã cảnh báo về nguy cơ bị chiếm đoạt thông tin, tài liệu song người dùng lại chủ quan, thiếu kiến thức, ý thức bảo mật nên tạo điều kiện thuận lợi cho tin tặc và các đối tượng xấu tấn công, chiếm đoạt, thu thập hình ảnh, dữ liệu cá nhân sử dụng vào mục đích bất chính.

- *Tình trạng lan tràn, phổ biến các thông tin giả, thông tin sai sự thật trên mạng.* Theo thống kê của Trung tâm Xử lý tin giả Việt Nam (VAFC) thuộc Bộ Thông tin và Truyền thông, chỉ 6 tháng sau khi thành lập (năm 2021), Trung tâm đã nhận được hơn 1,1 nghìn lượt báo cáo tin giả. Sau quá trình xác minh, Trung tâm đã công bố dán nhãn 38 tin giả, tin sai sự thật, trong đó có nhiều tin gây hoang mang dư luận, ảnh hưởng nghiêm trọng đến các hoạt động kinh tế, xã hội, tiềm ẩn nguy cơ gây mất an ninh, trật tự ở trong nước.

Tin giả gây hậu quả, thiệt hại về nhiều mặt. *Về chính trị,* những thông tin xuyên tạc chủ trương, chính sách của Đảng, Nhà nước; những hành vi giả mạo website, blog của cơ quan Đảng, Nhà nước, các đồng chí lãnh đạo để đăng tin có thể ảnh hưởng trực tiếp đến hoạt động quản lý, điều hành xã hội; gây mất uy tín, ảnh hưởng đến hình ảnh của Việt Nam trên trường quốc tế; làm giảm niềm tin của quần chúng nhân dân vào sự lãnh đạo của Đảng, sự quản lý, điều hành của bộ máy nhà nước. Thực tế, trên mạng xã hội Facebook đã từng xuất hiện tài khoản giả mạo mang tên *"Ban Tuyên giáo Trung ương Đảng Cộng sản Việt Nam",* cùng hàng trăm blog giả mạo các đồng chí lãnh đạo Đảng, Nhà nước để đăng tin nhằm định hướng dư luận, gây nhiễu loạn thông tin, khiến cư dân mạng không phân biệt được thông tin thật, giả. *Về kinh tế,* tin giả gây thiệt hại trực tiếp về kinh tế, có thể làm đình trệ hoạt động sản xuất, khả năng tiêu thụ sản phẩm của doanh nghiệp. Tin giả cũng có thể làm ảnh hưởng đến hoạt động bình thường của các cơ quan, tổ chức, doanh nghiệp kinh tế, ảnh hưởng đến tâm lý của nhà đầu tư, tác động tiêu cực đến hoạt động của các loại thị trường (nhất là thị trường tài chính, chứng khoán, thị trường bất động sản,…). Điển hình như Sau khi cơ quan Công an khởi tố, bắt tạm giam lãnh đạo tập đoàn FLC, Tân Hoàng Minh, xuất hiện nhiều tin giả, tin sai sự thật liên quan đến thị trường chứng khoán; các từ khóa như "vỡ nợ", "sẽ bị bắt" được chia sẻ nhiều trên MXH, nhiều bài viết được cả các thế lực thù địch chia sẻ như "lộ danh sách 12 ông lớn bất động sản sắp bị thanh tra, FLC, Tân Hoàng Minh, giờ đến ai"; "sau FLC, Tân Hoàng Minh sẽ đến ai", gây hoang mang cho nhà đầu tư, dẫn đến bán tháo cổ phiếu, ảnh hưởng nghiêm trọng đến thị trường. Chỉ tính 3 phiên giao dịch ngày 7,8,12/4/2022, VN Index giảm mạnh dưới mức 1.500 điểm, vốn hóa HOSE mất 265.700 tỷ đồng (tương đương 11,5 tỷ USD).

Về xã hội, tin giả có thể tạo dư luận tiêu cực, gây hoang mang trong quần chúng nhân dân; ảnh hưởng đến tâm lý, hoạt động bình thường của từng cá nhân, ảnh hưởng trực tiếp đến uy tín, danh dự, nhân phẩm, thậm chí đẩy họ tới những hành vi tiêu cực. Tin giả cũng gây chia rẽ trong cộng đồng, hình thành các nhóm dư luận trái chiều, tiềm ẩn nguy cơ dẫn đến những xung đột xã hội tiêu cực, ảnh hưởng trực tiếp đến an ninh, trật tự. Thực tế những thông tin như "máy bay rơi tại sân bay Nội Bài", "trẻ em nhập viện vì ngộc độc thịt lợn có chứa thuốc an thần", làm giả văn bản chỉ đạo của Ủy ban nhân dân Đà Nẵng nhằm tạo cơn sốt đất,… đã gây ra những bất ổn trong đời sống xã hội. Hay nổi bật thời gian qua là tin giả liên quan đến dịch bệnh Covid19, nhiều thông tin sai sự thật về tình hình dịch bệnh và các biện pháp phòng, chống dịch bệnh của Chính phủ đã được tạo ra và phát tán trên mạng xã hội khiến một bộ phận người dân cảm thấy bất an, nhiều người còn chuẩn bị các phương án tích trữ lương thực, thực phẩm, di chuyển về quê để tránh "phong tỏa",… gây phức tạp về an ninh, trật tự cũng như hiệu quả công tác chống dịch của các cơ quan chức năng. *Đối với an ninh quốc gia*, các thế lực thù địch, phần tử cơ hội, cực đoan, chống đối tăng cường hoạt động tán phát tin giả xuyên tạc tình hình kinh tế, chính trị, xã hội ở trong nước từ đó chia rẽ, khoét sâu thêm mâu thuẫn giữa người dân và chính quyền; tập trung khai thác, tán phát tin giả những những sự kiện chính trị thu hút sự quan tâm của quần chúng nhân dân, các vấn đề gây bức xúc trong dư luận, ảnh hưởng đến quyền lợi, tâm tư, tình cảm của đông đảo quần chúng nhân dân để kêu gọi, kích động người dân tập trung đông người, biểu tình, gây rối an ninh, trật tự. Điển hình như những tin giả, tin sai sự thật liên quan đến ngân hàng TMCP Sài Gòn (SCB) sau khi bà Trương Mỹ Lan, Chủ tịch Hội đồng quản trị Công ty cổ phần Tập đoàn Vạn Thịnh Phát bị cơ quan Công an bắt tạm giam. Các thông tin trên đã dẫn đến việc người dân ồ ạt rút tiền, làm thủ tục rút tiền trước thời hạn tại ngân hàng SCB, gây ra tình trạng tê liệt cục bộ và ảnh hưởng xấu đến tâm lý của người dân cả nước đối với hoạt động của các ngân hàng TMCP. Lợi dụng vụ việc trên, các đối tượng cũng tạo lập nhiều nhóm facebook, zalo thu hút hàng ngàn người tham gia, kêu gọi đi biểu tình tại các điểm giao dịch của ngân hàng SCB, tiềm ẩn nguy cơ gây mất an ninh, trật tự.

- *Sự lệ thuộc cả phần cứng, phần mềm và công nghệ bảo mật, bảo đảm an ninh hệ thống thông tin của Việt Nam vào nước ngoài;* tình trạng lạm dụng các phần mềm, công nghệ bảo mật hệ thống không có bản quyền, nhiều lỗ hổng, nguy cơ gây mất an ninh thông tin cao diễn ra khá phổ biến. Hầu hết công nghệ, kỹ thuật và các dịch vụ mạng được sử dụng rộng rãi hiện nay ở Việt Nam đều do nước ngoài cung cấp, có máy chủ đặt tại nước ngoài. Thiết bị, công nghệ nhiều rủi ro của nước ngoài đã thâm nhập sâu vào hệ thống mạng lõi như tổng đài, thiết bị quản lý, định vị thuê bao, hệ thống quản lý - điều hành mạng. Trong khi đó, công nghệ bảo mật của Việt Nam phần lớn lạc hậu, chưa được quan tâm đầu tư đúng mức. Điều này

tiềm ẩn nguy cơ mất kiểm soát an ninh thông tin, hệ thống thông tin dễ bị tấn công, xâm nhập từ nhiều hướng.

Hiện nay, linh kiện điện tử, thiết bị công nghệ thông tin, đặc biệt là thiết bị thông minh giá rẻ tại Việt Nam đều có nguồn gốc từ nước ngoài, chứa nhiều lỗ hổng bảo mật hoặc cài sẵn các tài khoản truy cập "cửa hậu" (backdoor), khiến Việt Nam luôn nằm trong danh sách các quốc gia bị ảnh hưởng bởi các "mạng máy tính ma" (botnet) lớn nhất thế giới.

- Xuất hiện nhiều lỗ hổng, điểm yếu dễ bị tấn công trên hệ thống thông tin, nhất là hệ thống mạng lõi, hệ thống thông tin quan trọng về an ninh quốc gia; tình trạng lộ, mất bí mật nhà nước qua hệ thống thông tin, 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. Qua rà soát cho thấy, hầu hết các cổng thông tin, trang tin điện tử của cơ quan Đảng, Nhà nước Việt Nam tồn tại lỗ hổng bảo mật, hàng triệu địa chỉ IP của Việt Nam thường xuyên nằm trong danh sách đen của các tổ chức quốc tế; nhiều camera IP tồn tại các điểm yếu và lỗ hổng bảo mật có thể bị khai thác, lợi dụng.

Cùng với đó, do chủ quan, sơ hở, thiếu sót trong bảo vệ bí mật nhà nước, một số cơ quan, tổ chức, cán bộ, đảng viên đã đăng tải, trả lời phỏng vấn, gửi, nhận, soạn thảo, lưu giữ, thông tin thuộc phạm vi bí mật nhà nước qua các phương tiện truyền thông đại chúng, mạng xã hội, máy tính có kết nối Internet,… dẫn đến lộ, mất bí mật. Từ 2016 đến 2023, cả nước xảy 608 vụ lộ, mất bí mật nhà nước với hơn 2.160 tin, tài liệu khác nhau, trong đó hình thức lộ, mất bí mật nhà nước chủ yếu là qua các phương tiện thông tin, truyền thông, nhất là qua mạng Internet (chiếm tỷ lệ 75%). Tình trạng khai thác, sử dụng trái phép cơ sở dữ liệu, thông tin cá nhân người dùng diễn biến phức tạp, nhất là hoạt động của các doanh nghiệp, tổ chức, cá nhân mua bán, sử dụng trái phép thông tin cá nhân các thuê bao điện thoại di động; tình trạng khai thác, sử dụng trái phép thông tin, hình ảnh của tổ chức, cá nhân để quảng cáo vì mục đích thương mại; facebook và google thông qua các dịch vụ, ứng dụng thu thập trái phép hình ảnh, thông tin cá nhân của người dùng,… Tháng 3/2018, Facebook đã để lộ dữ liệu cá nhân để một nhà phát triển bán lại cho Công ty Cambridge Analityca, dẫn tới 87 triệu dữ liệu thông tin người dùng bị lộ, trong đó có 427.466 tài khoản của người dùng Việt Nam. Cục An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao thuộc Bộ Công an đã phát hiện, xử lý nhiều vụ việc mua bán trái phép dữ liệu cá nhân. Nổi bật là phát hiện, xử lý đối tượng rao bán trái phép dữ liệu của hơn 25 triệu người cài đặt ứng dụng "Sổ sức khỏe điện tử", rao bán thông tin của 35,6 triệu khách hàng Tập đoàn Điện lực Việt Nam; phát hiện diễn đàn trên mạng rao bán 17GB dữ liệu là ảnh chụp căn cước công dân có gắn chip mới được cấp phát của người dân ở Việt Nam,…

- Ý thức người dùng về các nguy cơ gây mất an ninh, an toàn thông tin yếu kém; năng lực tự chủ, tự bảo vệ trước các thông tin xấu, độc hại thấp, dễ bị kích

động bởi các luận điệu sai trái trên không gian mạng. Nhiều thông tin giả, thông tin gây nhiễu, thông tin xấu, độc hại dễ dàng được người dân tiếp nhận, chia sẻ.

- *Chính sách, pháp luật chưa đồng bộ, chưa tạo được hành lang pháp lý vững chắc cho đảm bảo an ninh thông tin,* chưa có cơ chế thống nhất trong đấu tranh chống thông tin xấu, độc hại, phản bác các quan điểm sai trái, thù địch. Trong khi đó, đây là vấn đề mà hầu hết các quốc gia trên thế giới đang đặc biệt quan tâm. Trung Quốc xây dựng hệ thống tường lửa quốc gia, kiểm soát thông tin xấu, độc hại trên Internet bằng cách phát hiện và ngăn chặn ngay khi chúng xâm nhập vào không gian mạng của Trung Quốc. Singapore, Malaysia lập các trang thông tin điện tử để công chúng kiểm tra tính xác thực của thông tin. Indonesia thành lập cơ quan mã hóa và an ninh mạng quốc gia nhằm ngăn chặn tin tức giả trên các phương tiện truyền thông. Philippin ban hành đạo luật mới xác định việc truyền bá thông tin xấu, độc hại là tội hình sự và bị xử phạt nghiêm ngặt hơn.

- *Sự thiếu hụt nghiêm trọng nguồn lực đảm bảo an ninh mạng, cả về con người, tài chính và đầu tư công nghệ phục vụ quản trị, điều hành hệ thống mạng.* Việt Nam hiện chưa có cơ sở đào tạo chuyên sâu về an ninh mạng. Ngày 14/01/2014, Thủ tướng Chính phủ đã phê duyệt đề án "Đào tạo và phát triển đội ngũ chuyên gia an toàn, an ninh thông tin đến 2020" song mục tiêu của đề án chỉ nhằm đáp ứng yêu cầu của các cơ quan, tổ chức, doanh nghiệp về bảo đảm an ninh, an toàn thông tin, chưa có định hướng về đào tạo chuyên gia an ninh mạng, chưa đáp ứng được thực tế nhiệm vụ bảo vệ an ninh quốc gia trên không gian mạng, bảo đảm an toàn hệ thống mạng thông tin trọng yếu quốc gia. Theo Vietnam Works, Việt Nam hiện tại thiếu hụt khoảng 78.000 nhân lực IT mỗi năm và đến 2022 đã thiếu hơn 700.000 nhân lực IT.

Thực tế nêu trên đã làm xuất hiện nhiều nguy cơ đe dọa đến an ninh mạng của Việt Nam ở cả bên trong và bên ngoài, ảnh hưởng tiêu cực đến phòng, chống tội phạm sử dụng công nghệ cao và tệ nạn xã hội ở Việt Nam. Ở trong nước, trước hết là nguy cơ tụt hậu về công nghệ, lệ thuộc vào công nghệ của nước ngoài, nhất là hệ thống mạng lõi; sự lệ thuộc vào phần mềm hệ thống, dịch vụ thông tin của nước ngoài (nhất là dịch vụ mạng xã hội) dẫn tới mất chủ quyền nội dung số, tài nguyên thông thông tin về các công ty công nghệ nước ngoài ngày càng nghiêm trọng hơn; các đối tượng cơ hội, chống đối chính trị trong nước, nhất là các đối tượng chống đối trong tôn giáo triệt để sử dụng mạng xã hội tán phát thông tin gây rối nội bộ, kích động biểu tình, bạo loạn.

Ở bên ngoài, các nước có chính sách thù địch với chủ nghĩa xã hội, có ý đồ bành trướng bá quyền, gây ảnh hưởng với Việt Nam triệt để sử dụng không gian mạng để tác động, can thiệp nội bộ, hướng lái chính sách, thao túng dư luận, thúc đẩy "cách mạng màu" ở Việt Nam; xâm phạm độc lập, chủ quyền quốc gia trên không gian mạng, tiến hành chiến tranh thông tin đối với Việt Nam. Các tổ chức phản động lưu vong, khủng bố tăng cường hoạt động tấn công, phá hoại hệ thống

thông tin quan trọng về an ninh quốc gia; sử dụng không gian mạng để tán phát thông tin xấu, độc hại, kích động biểu tình, bạo loạn; hình thành các hội, nhóm, các tổ chức chính trị đối lập,… Các tổ chức tin tặc, tổ chức tội phạm thực hiện các cuộc tấn công mạng tự phát, đơn lẻ hoặc có chủ đích nhằm vào hệ thống thông tin trọng yếu quốc gia, làm tê liệt, gây gián đoạn hoạt động lãnh đạo, chỉ đạo, điều hành, quản lý kinh tế-xã hội của các cơ quan Đảng, Nhà nước, xâm hại trực tiếp đến quyền, lợi ích hợp pháp của tổ chức, cá nhân.

III. MỘT SỐ KHUYẾN CÁO VỚI HỌC SINH, SINH VIÊN TRONG BẢO VỆ AN NINH MẠNG VÀ PHÒNG, CHỐNG TỘI PHẠM SỬ DỤNG CÔNG NGHỆ CAO

1. Nâng cao nhận thức, ý thức chấp hành pháp luật về bảo vệ an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao.

a. Chấp hành nghiêm các hành vi bị cấm được quy định tại điều 8 Luật An ninh mạng.

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

+ Đăng tải các thông tin có nội dung vi phạm pháp luật: (1) 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); (2) 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). (3) Thông tin trên không gian mạng có nội dung làm nhục, vu khống (bao gồm: Xúc phạm nghiêm trọng danh dự, uy tín, nhân phẩm của người khác;Thông tin bịa đặt, sai sự thật xâm phạm danh dự, uy tín, nhân phẩm hoặc gây thiệt hại đến quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân khác). (4) Thông tin trên không gian mạng có nội dung xâm phạm trật tự quản lý kinh tế (bao gồm: Thông tin bịa đặt, sai sự thật về sản phẩm, hàng hóa, tiền, trái phiếu, tín phiếu, công trái, séc và các loại giấy tờ có giá khác; thông tin bịa đặt, sai sự thật trong lĩnh vực tài chính, ngân hàng, thương mại điện tử, thanh toán điện tử, kinh doanh tiền tệ, huy động vốn, kinh doanh đa cấp, chứng khoán); (5) Thông tin trên không gian mạng có nội dung bịa đặt, 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.

+ Thực hiện hành vi gián điệp mạng; xâm phạm 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 bao gồm: (1) Chiếm đoạt, mua bán, thu giữ, cố ý làm lộ 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 gây ảnh hưởng đến danh dự, uy tín, nhân phẩm, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân. (2) Cố ý xóa, làm hư hỏng, thất lạc, thay đổi 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 được truyền đưa, lưu trữ trên không gian mạng. (3) Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa biện pháp kỹ thuật được xây dựng, áp dụng để 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. (4) Đưa lên không gian mạng những 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 trái quy định của pháp luật. (5) Cố ý nghe, ghi âm, ghi hình trái phép các cuộc đàm thoại. (6) Hành vi khác cố ý xâm phạm 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.

+ 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.

- Không 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.

- Không 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.

- Không 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.

b. Thực hiện tốt các quy định trong Bộ quy tắc ứng xử trên mạng xã hội.

- Các quy tắc ứng xử chung:

Quy tắc tôn trọng, tuân thủ pháp luật: Tuân thủ pháp luật Việt Nam, tôn trọng quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Quy tắc lành mạnh: Hành vi, ứng xử trên mạng xã hội phù hợp với các giá trị đạo đức, văn hóa, truyền thống tốt đẹp của dân tộc Việt Nam.

Quy tắc an toàn, bảo mật thông tin: Tuân thủ các quy định và hướng dẫn về bảo vệ an toàn và bảo mật thông tin.

Quy tắc trách nhiệm: Chịu trách nhiệm về các hành vi, ứng xử trên mạng xã hội; phối hợp với các cơ quan chức năng để xử lý hành vi, nội dung thông tin vi phạm pháp luật.

- Quy tắc ứng xử cho cá nhân:

Tìm hiểu và tuân thủ các điều khoản hướng dẫn sử dụng của nhà cung cấp dịch vụ mạng xã hội trước khi đăng ký, tham gia mạng xã hội.

Nên sử dụng họ, tên thật cá nhân, tên hiệu thật của tổ chức, cơ quan và đăng ký với nhà cung cấp dịch vụ để xác thực tên hiệu, địa chỉ trang mạng, đầu mối liên lạc khi tham gia, sử dụng mạng xã hội.

Thực hiện biện pháp tự quản lý, bảo mật tài khoản mạng xã hội và nhanh chóng thông báo tới các cơ quan chức năng, nhà cung cấp dịch vụ khi tài khoản cá nhân bị mất quyền kiểm soát, bị giả mạo, lợi dụng và sử dụng vào mục đích không lành mạnh, ảnh hưởng đến ANQG và TTATXH, ảnh hưởng đến quyền và lợi ích hợp pháp của tổ chức, cá nhân.

Chia sẻ thông tin có nguồn chính thống, đáng tin cậy.

Có các hành vi, ứng xử phù hợp với những giá trị đạo đức, văn hóa, truyền thống của dân tộc Việt Nam; không sử dụng từ ngữ gây thù hận, kích động bạo lực, phân biệt vùng miền, giới tính, tôn giáo.

Không đăng tải những nội dung vi phạm pháp luật, các thông tin xúc phạm danh dự, nhân phẩm ảnh hưởng đến quyền và lợi ích hợp pháp của các tổ chức, cá nhân khác; sử dụng ngôn ngữ phản cảm, vi phạm thuần phong mỹ tục; tung tin giả, tin sai sự thật; quảng cáo, kinh doanh dịch vụ trái phép,… gây bức xúc trong dư luận xã hội, ảnh hưởng đến trật tự an toàn xã hội.

Khuyến khích sử dụng mạng xã hội để tuyên truyền, quảng bá về đất nước, con người, văn hóa tốt đẹp của Việt Nam, chia sẻ thông tin tích cực, những tấm gương người tốt, việc tốt.

Vận động người thân, gia đình, bạn bè, những người xung quanh tham gia giáo dục, bảo vệ trẻ em, trẻ vị thành niên sử dụng mạng xã hội một cách an toàn, lành mạnh.

2. Kỹ năng sử dụng mạng Internet, mạng xã hội an toàn

- Đảm bảo an toàn cho thiết bị:

Cài đặt xác thực đăng nhập thiết bị bằng mật khẩu, sinh trắc học (vân tay, khuôn mặt) hoặc thiết bị vật lý (token key).

Thường xuyên cập nhật hệ điều hành và phần mềm.

Thận trọng khi cài đặt các phần mềm mới, chỉ cài những ứng dụng thật cần thiết. Trước khi cài đặt cần xem xét kỹ các quyền mà ứng dụng yêu cầu, chỉ cài ứng dụng với những quyền phù hợp với chức năng của ứng dụng, hạn chế cài các ứng dụng yêu cầu quyền nhạy cảm (truy cập danh bạ, tin nhắn, cuộc gọi, camera, vị trí, bộ nhớ,…). Chỉ cài ứng dụng từ chợ ứng dụng chính thức hoặc tải từ trang chủ của hãng (các công ty có uy tín).

Không cài các ứng dụng, phần mềm có nguồn gốc không rõ ràng; phần mềm đã chỉnh sửa (crack).

Không cài các tiện ích (addons), phần mở rộng (extensions) của trình duyệt web không rõ nguồn gốc, có các tính năng thu thập cookie, token, mật khẩu của mạng xã hội, không ghi nhớ mật khẩu trong trình duyệt.

Bảo mật chặt chẽ tài khoản quản lý thiết bị (Apple, Google. Microsoft).

Cẩn trọng khi sử dụng dịch vụ lưu trữ và đồng bộ trên đám mây.

Sử dụng tường lửa, các phần mềm bảo mật, phần mềm diệt virus: Windows Defender, AVG Antivirus, Kaspersky Internet Security, 360 Mobile Security,…

Phòng, chống tấn công, xâm nhập, câu nhử: Không cài đặt, mở các file, truy cập các link không rõ nguồn gốc; trường hợp bắt buộc phải mở phải có giải pháp đảm bảo an ninh, an toàn (rà quét virus, sử dụng máy ảo, máy trung gian không kết nối mạng,…); hạn chế sử dụng Internet công cộng trên các thiết bị.

- Đảm bảo an toàn cho tài khoản mạng xã hội:

Sử dụng mật khẩu mạnh (mật khẩu có dài trên 8 ký tự, nên bao gồm chữ thường, chữ hoa, số, ký tự đặc biệt không nằm trong danh sách các mật khẩu thường sử dụng, đã bị lộ trên Internet).

Thiết lập xác thực 2 bước cho tài khoản (facebook, email,…), có thể gửi mã xác thực (OTP) thông qua SMS hoặc ưu tiên sử dụng mã 2FA để xác thực email hoặc sử dụng phần mềm sinh mã tự động (Google Authenticator, Microsoft Authenticator,…) hoặc sử dụng email khôi phục là tài khoản gốc của cá nhân để hỗ trợ khôi phục, bảo mật tài khoản.

Bảo mật thông tin, tài khoản phục hồi (email, số điện thoại): không công khai số điện thoại, email, ngày tháng năm sinh dùng để đăng ký tài khoản Facebook.

Thiết lập cài đặt bảo mật, quyền riêng tư: cài đặt xác thực 2 lớp hoặc đặt chế độ riêng tư cho các thông tin cần bảo mật (số điện thoại, email).

Tạo cảnh báo đăng nhập (Login Alerts) để nhận thông báo mỗi khi tài khoản được đăng nhập từ một máy tính hoặc thiết bị lạ.

Tạo xét duyệt đăng nhập (Login Approvals): khi kích hoạt tính năng này, mỗi lần đăng nhập vào tài khoản Facebook hay Gmail từ một thiết bị, trình duyệt khác hoặc chưa từng sử dụng trước đó, Facebook, Gmail sẽ gửi một đoạn mã xác thực hoặc bật cửa sổ cảnh báo (trên thiết bị tin cậy mà người dùng đang sử dụng), người dùng phải nhập mã hoặc chọn đồng ý để xác thực và sử dụng.

Thiết lập chọn bạn bè để liên hệ khi không đăng nhập được nhằm mục đích khôi phục lại mật khẩu Facebook.

Thoát các phiên đăng nhập tài khoản từ xa trong trường hợp quên không đăng xuất trên một thiết bị khác.

Luôn để ý các thông báo đăng nhập, nếu có bất thường cần hủy ngay phiên đăng nhập đó.

Thường xuyên kiểm tra địa điểm đăng nhập và nhật ký hoạt động để phát hiện các hoạt động bất thường.

- Đảm bảo an toàn khi kết nối:

Thận trọng khi đăng nhập tài khoản từ các ứng dụng, trình duyệt không tin cậy.

Thận trọng với các trào lưu mới nổi trên mạng xã hội mà yêu cầu click và đăng nhập vào đường link hoặc sử dụng app nào đó không đáng tin cậy.

Tránh truy cập wifi công cộng. Tin tặc có thể giả mạo mạng wifi tương tự như wifi công cộng hiện tại để lôi kéo người dùng đăng nhập. Sau đó bằng các công cụ biên dịch chúng có thể đọc được dữ liệu trao đổi giữa thiết bị di động và mạng wifi.

Tránh đăng nhập ở nhiều thiết bị, sử dụng nhiều đường truyền kết nối Internet khác nhau.

3. Kỹ năng nhận diện tin giả, tin sai sự thật trên Internet, mạng xã hội.

Tin giả có thể được hiểu là những thông tin không có thật, không chính xác, chưa được kiểm chứng, kiểm duyệt, xuất hiện sai lệch về nội dung, được phát tán rộng rãi qua nhiều hình thức, phương tiện khác nhau, xâm hại trực tiếp đến lợi ích hợp pháp của Nhà nước, quyền và lợi ích hợp pháp của các cơ quan, tổ chức và cá nhân.

Tin giả bao gồm: (1) Những thông tin hoàn toàn không có thật, tin bịa đặt, vu khống được lan truyền trong xã hội và trên không gian mạng. (2) Những thông tin có một phần sự thật nhưng không hoàn toàn chính xác, bị xuyên tạc, bóp méo được lan truyền trong xã hội và trên không gian mạng.

Cách nhận biết tin giả:

- Tăng cường sự đề phòng, tính cảnh giác của bản thân khi tiếp xúc với thông tin được lan truyền trên không gian mạng. Luôn có quan điểm tham khảo khi sử dụng thông tin trên không gian mạng, nhất là thông tin được chia sẻ bởi mạng xã hội, chủ thể không rõ nguồn gốc, không xác thực.

- Nếu là những thông tin đáng chú ý, thuộc lĩnh vực cần quan tâm thì cần chú ý tiêu đề bài viết. Tin giả thường có tiêu đề hấp dẫn, giật gân, viết in hoa kèm dấu ký tự mang tính chất khẳng định, thường có vẻ khó xảy ra trong thực tế nhưng được viết dưới dạng khẳng định để thu hút sự chú ý của người đọc.

- Kiểm tra đường dẫn liên kết. Đường dẫn URL chứa tin giả thường giả mạo gần giống các trang tin chính thống. Cần kiểm tra kỹ mục "Liên hệ" hoặc "Giới thiệu" trên trang tin để tìm kiếm thông tin về cá nhân hoặc tổ chức đứng sau, xác định mức độ tin tưởng thông qua các thông tin được đề cập như: Chức danh, chức vụ, học hàm, học vị, mức độ phản hồi của người dùng, tính xác thực của địa chỉ.

- Kiểm tra cấu trúc ngữ pháp, thể thức văn bản, hình ảnh được sử dụng. Tin giả thường không được chú trọng về cấu trúc ngữ pháp, thể thức văn bản, dễ có lỗi chính tả và ngữ pháp, không thống nhất. Hình ảnh sử dụng trong bài viết đa phần là ảnh trên mạng hoặc được chỉnh sửa cho phù hợp với nội dung nguồn tin. Cần kiểm tra xem ảnh có tồn tại trên không gian mạng thông qua tính năng "Search Google for image".

- Kiểm tra mốc thời gian, luận cứ, luận chứng được sử dụng trong bài viết. Tin giả được biên soạn và định dạng mốc thời gian không trùng với thực tế, do đó, cần xem kỹ các mốc thời gian, sự kiện có trong nội dung tin và thời gian đăng tải. Về các luận cứ, luận chứng trong bài viết, thông thường các tin giả được tạo ra được dựa trên một câu chuyện, tình tiết có thực nhưng được làm giả ở những nội dung quan trọng nhất.

- Luôn kiểm tra chéo thông tin với các website uy tín khác.

4. Kỹ năng nhận diện và phòng ngừa tội phạm sử dụng không gian mạng lừa đảo chiếm đoạt tài sản.

Các thủ đoạn thường gặp trong các vụ sử dụng không gian mạng để lừa đảo, chiếm đoạt tài sản: (1). Giả danh (Công an, Viện kiểm sát, Tòa án) để hù doạ, thông báo phạt nguội, nâng cấp tài khoản thực hiện các dịch vụ công,… (2) Bẫy tình (yêu đương qua mạng) gửi gói quà, yêu cầu đóng phí. (3) Hack Zalo, Facebook (giả người thân, bạn bè..) để vay mượn tiền. (4) Tuyển nhân viên bán đơn hàng trên mạng. (5) Lập sàn giao dịch tiền ảo (ngoại hối, chứng khoán, bitcon..) để lừa đảo. (6) Thông báo trúng thưởng, bán hàng giá rẻ trên mạng… sau đó chiếm đoạt tài sản. (7) Cung cấp đường link mua, bán hàng trực tuyến, chuyển tiền làm từ thiện,… để lừa đảo chiếm đoạt tài sản. (8) Giả nhân viên ngân hàng nâng cấp APP, nhân viên nhà mạng nâng cấp sim 4G, giả mạo cán bộ Viễn thông, Cục Bưu chính yêu cầu cung cấp các thông tin.. để lừa đảo chiếm đoạt tài sản. (9) Giả mạo cơ quan Bảo hiểm xã hội, chuyển tiền làm từ thiện… nhằm chiếm đoạt tài sản. (10) Vay tiền qua AP trên mạng, gọi điện quấy rối, khủng bố điện thoại người vay, người thân, bạn bè của người vay,…

Khi gặp các tình huống trên, phương hướng xử lý chung là: (1) Không ham

muốn những tài sản, vật chất "tự nhiên mà có". (2) Không cung cấp thông tin cá nhân, mã OTP cho người khác. (3) Không nhấp vào những đường link lạ trên tin nhắn và mạng xã hội. (4) Không chuyển tiền cho người lạ, gọi điện thoại xác thực trước khi chuyển. (5) Không thực hiện bất cứ yêu cầu chuyển tiền nào từ người tự xưng là các cơ quan chức năng. (6) Luôn trao đổi, tìm kiếm lời khuyên, tư vấn từ người thân, bạn bè.

Xử lý một số tình huống cụ thể:

- Thủ đoạn: Kết bạn, làm quen trên mạng xã hội.

Đối tượng người nước ngoài hoặc giả làm người nước ngoài, sử dụng mạng xã hội như Facebook, Zalo,…kết bạn làm quen với người bị hại, dành nhiều thời gian trò chuyện tạo sự tin tưởng; Sau một thời gian thông báo gửi quà là tiền hoặc tài sản có giá trị lớn; Điện thoại người Việt Nam giả danh nhân viên sân bay, hải quan, thuế,… yêu cầu người bị hại nộp tiền để nhận được quà, tạo nhiều lý do để bị hại nộp tiền nhiều lần. Cắt đứt liên lạc khi hết nguồn tiền hoặc bị nghi ngờ.

Khuyến cáo: Có thể quen biết, kết bạn với người nước ngoài qua mạng xã hội nhưng không nên gửi, chuyển tiền để đóng các loại phí vào tài khoản do đối tượng cung cấp với bất cứ lý do gì.

- Thủ đoạn: Giả danh cán bộ Công an, Viện kiểm sát, tòa án, cơ quan nhà nước. Đối tượng thông báo bị hại liên quan đến vụ án đang điều tra, rồi nối máy đến đối tượng khác giả danh là người của cơ quan tư pháp để khai thác thông tin cá nhân và tài khoản ngân hàng. Đối tượng tự xưng là nhân viên bưu điện thông báo bị hại đang nợ tiền cước điện thoại hoặc có bưu phẩm lâu ngày không đến nhận. Đối tượng thông báo bị hại thiếu nợ tiền ngân hàng do người khác lấy CCCD đăng ký mở tài khoản ngân hàng. Điện thoại thông báo có giao dịch tiền vào tài khoản nhưng bị treo, yêu cầu cung cấp thông tin đăng nhập, mật khẩu và mã OTP để nhận tiền. Yêu cầu bị hại chuyển tiền vào tài khoản chỉ định để kiểm tra nguồn gốc rồi sẽ trả lại hoặc đe dọa nếu không chuyển sẽ bị bắt giam. Hướng dẫn bị hại tải phần mềm "Bộ Công an" giả mạo để cung cấp thông tin sau đó chiếm đoạt quyền sử dụng tài khoản,…

Khuyến cáo: Cơ quan Công an, Viện kiểm sát, Toà án không yêu cầu chuyển tiền vào tài khoản cá nhân vì bất cứ lý do gì. Mọi trường hợp đều làm việc tại trụ sở cơ quan nhà nước. Khi có số điện thoại lạ liên lạc thông báo có liên quan đến tội phạm và yêu cầu cung cấp thông tin cá nhân hoặc chuyển tiền thì tuyệt đối không chuyển, thông báo cho người thân, gia đình và trình báo với cơ quan Công an nơi gần nhất. Không cung cấp thông tin cá nhân cho người không quen biết, yêu cầu được làm việc trực tiếp.

- Thủ đoạn: Vay tiền qua App. Mạo danh ngân hàng, nhân viên ngân hàng, công ty tài chính đăng tải thông tin hỗ trợ vay tiền online, giải ngân nhanh trên mạng xã hội với thủ tục nhanh gọn, không cần thế chấp tài sản. Hướng dẫn người dân truy cập vào website hoặc ứng dụng điện thoại để làm thủ tục. Thông báo

người dân cung cấp sai thông tin nên hệ thống báo lỗi không thể giải ngân. Đề nghị bị hại nộp các khoản phí để làm lại thủ tục vay rồi chiếm đoạt số tiền.

Khuyến cáo: Không vay tiền online từ các ứng dụng không rõ nguồn gốc. Nếu có nhu cầu vay tiền thì liên hệ và đến trực tiếp ngân hàng, các tổ chức tín dụng gần nhất để được hỗ trợ. Tuyệt đối không cung cấp mã OTP cho người khác khi sử dụng tài khoản ngân hàng.

- *Thủ đoạn: Giả danh người thân nhờ chuyển tiền rồi chiếm đoạt.* Đối tượng lập tài khoản mạng xã hội hoặc chiếm đoạt quyền quản trị tài khoản mạng xã hội (hack) của người khác. Nhắn tin cho người thân, bạn bè trong danh sách liên lạc hỏi vay tiền hoặc nhờ chuyển tiền, khi người thân gọi lại bằng video thì hình ảnh nhoà hoặc nhiễu sau đó bị tắt ngay do mất sóng.

Khuyến cáo: Gọi điện trực tiếp cho người thân để xác minh trước khi chuyển tiền (gọi số sim, không gọi qua các ứng dụng mạng).

- *Thủ đoạn: Nhắn tin trúng thưởng.* Đối tượng sử dụng facebook, tin nhắn để gửi thông báo cho bị hại thông báo trúng thưởng tài sản hoặc tiền mặt có giá trị lớn. Yêu cầu người bị hại nạp tiền qua thẻ điện thoại hoặc chuyển qua tài khoản ngân hàng để làm thủ tục nhận thưởng; hướng dẫn truy cập vào các đường link gửi kèm để khai báo thông tin người nhận thưởng.

Khuyến cáo: Không thực hiện chuyển tiền hay nạp tiền qua thẻ điện thoại vì lý do nhận thưởng. Không truy cập vào các đường link được đính kèm trong các tin nhắn lạ, không thực hiện thao tác trên điện thoại theo cú pháp được hướng dẫn bởi người lạ. Tuyệt đối không cung cấp mã OTP cho người khác khi sử dụng tài khoản ngân hàng.

- *Thủ đoạn: Kinh doanh đa cấp qua các sàn giao dịch tiền ảo, sàn ngoại hối hoặc đầu tư đào tiền kỹ thuật số.* Đối tượng lập ra các website tài chính, ứng dụng có giao diện tương tự như sàn đầu tư tài chính quốc tế rồi lôi kéo người tham gia. Cam kết người chơi có thể rút vốn bất kỳ lúc nào, không cần đầu tư trí tuệ, thời gian, kêu gọi được thêm người sẽ có hoa hồng. Sau một thời gian sàn thông báo dừng hoạt động để bảo trì hoặc lỗi không truy cập được. Khách hàng không đăng nhập được để rút tiền hoặc mất hết tiền kỹ thuật số trong tài khoản.

Khuyến cáo: Không tham gia vào các sàn giao dịch tiền ảo, tiền ngoại hối khi mình không hiểu rõ, không có kiến thức về vấn đề này.

- *Thủ đoạn: Kiếm tiền online qua App.* Đối tượng lập ra các app kiếm tiền (như Pchome, Shopping Mail, Tailoc888…) mời tham gia trò chơi, giật đơn hàng. Người chơi nạp tiền lần 1, lần 2 (mỗi lần 500k đến 1,5 triệu đồng) sẽ được chuyển lại tài khoản liên kết và lãi ngay 20%. Từ lần 3 trở đi sẽ được báo trúng đơn hàng từ 20 triệu đồng trở lên và chuyển tài khoản lần nào mất tiền lần đó. Người chơi đăng ký tài khoản trên web, nạp tiền theo 9 mức từ 180.000 đến 99.000.000đ sau đó mua các gói đầu tư từ 180.000đ đến 540.000đ để hưởng lãi suất 20% - 55% mỗi ngày, một thời gian sau đối tượng đánh sập hệ thống và chiếm đoạt tiền.

Khuyến cáo: Không tham gia vào các App kiếm tiền online.

- *Thủ đoạn: Bán hàng lừa đảo.* Đối tượng giả dạng nhân viên bán hàng chào mua các loại sản phẩm. Yêu cầu đặt cọc trước hôm sau sẽ giao hàng sau đó chiếm đoạt số tiền trên không còn liên lạc được nữa. Đối tượng quảng bá sản phẩm trên mạng, thu hút nhiều người theo dõi, nhiều lượt like, nhiều bình luận,… nhưng khi chuyển hàng không đảm bảo chất lượng.

Khuyến cáo: Khi trao đổi, mua bán trực tuyến qua các trang mạng xã hội phải tìm hiểu rõ nguồn gốc, hạn chế mua các mặt hàng có giá trị lớn. Lựa chọn phương thức kiểm tra hàng xong mới trả tiền.

- *Thủ đoạn: Tuyển cộng tác viên online.* Đối tượng mạo danh nhân viên của các trang thương mại điện tử để lôi kéo cộng tác viên bán hàng online với hoa hồng hấp dẫn. Yêu cầu cộng tác viên phải thanh toán tiền đơn hàng trước mới nhận được tiền gốc và hoa hồng. Thanh toán cho cộng tác viên từ 1 - 3 đơn hàng có giá trị thấp. Dụ dỗ, mời cộng tác viên tham gia, chuyển khoản để mua các đơn hàng có giá trị cao rồi chiếm đoạt tài sản.

Khuyến cáo: Nên kiểm tra kỹ các thông tin trước khi nhận làm cộng tác viên hoặc trước khi chuyển tiền.

- *Thủ đoạn: Gọi điện thoại mời đổi sim 4G.* Đối tượng mạo danh nhân viên chăm sóc khách hàng, gợi ý và yêu cầu bị hại bấm dãy số **21* số điện thoại * hoặc nhắn tin theo cú pháp DSxxxx để được đổi sim 4G với ưu đãi hấp dẫn. Đây là cách chuyển cuộc gọi và đổi sim sang phôi trắng, nếu làm theo sẽ mất quyền kiểm soát số điện thoại. Đối tượng sử dụng số điện thoại chiếm đoạt được để thao tác chuyển tiền trong tài khoản, ví điện tử của người bị hại.

Khuyến cáo: Nếu có nhu cầu đổi sim 4G thì ra trực tiếp cửa hàng để thực hiện.

- *Thủ đoạn: Gọi điện hướng dẫn cài đặt ứng dụng VneID và các ứng dụng khác theo yêu cầu của cơ quan Công an hoặc cơ quan nhà nước có thẩm quyền.* Lợi dụng việc nhiều người dân chưa nắm bắt đầy đủ thông tin liên quan đến cài đặt ứng dụng VneID và kích hoạt tài khoản định danh điện tử, các đối tượng lừa đảo giả danh cán bộ Công an phường, xã gọi điện thoại cho nạn nhân hẹn đến trụ sở để đồng bộ định danh điện tử hoặc đề nghị nạn nhân cài đặt qua mạng. Sau đó, đối tượng gửi cho nạn nhân đường link truy cập và tải một ứng dụng có tên, logo và giao diện giống ứng dụng VneID. Quá trình cài đặt , ứng dụng này sẽ thu thập dữ liệu trong điện thoại của nạn nhân cũng như những thông tin sinh trắc học, tin nhắn, danh bạ từ đó tấn công, chiếm quyền điều khiển tài khoản ngân hàng và chiếm đoạt tiền của nạn nhân.

Khuyến cáo: Cơ quan Công an và các cơ quan chức năng khác không làm việc hoặc yêu cầu người dân cung cấp thông tin qua điện thoại.

Cơ quan Công an chỉ hỗ trợ kích hoạt định danh điện tử trực tiếp cho người dân, không hướng dẫn kích hoạt qua điện thoại. Chỉ cài đặt các ứng dụng từ nguồn chính thống trên App Store (đối với hệ điều hành IOS) và CH Play (đối với hệ

điều hành Adroid). Tuyệt đối không cài đặt, kích hoạt ứng dụng từ các nguồn khác. Không chia sẻ thông tin tài khoản định danh điện tử (mật khẩu ứng dụng, mật khẩu tài khoản,…) cho người khác. Chỉ cung cấp thông tin trên ứng dụng cho cơ quan chức năng có thẩm quyền khi làm việc trực tiếp và có yêu cầu của cơ quan chức năng có thẩm quyền. Không bật chế độ cài đặt ứng dụng từ nguồn không xác định trên điện thoại di động hoặc cài dặt các ứng dụng, phần mềm không rõ nguồn gốc có nguy cơ mất an toàn thông tin, Tuyệt đối không cấp quyền truy cập vào danh bạ, tin nhắn, định vị, thư mục ảnh cho các ứng dụng lạ, ứng dụng không chính thống.

- *Thủ đoạn: lừa đảo lấy lại tiền bị lừa đảo.* Giả mạo các đơn vị chuyên trách bảo vệ an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao của Bộ Công an, mạo danh các công ty luật, luật sư quảng cáo hỗ trợ người dân lất lại tiền bị lừa đảo. Các trang web này lồng ghép quảng cáo các dịch vụ tiếp nhận hồ sơ, lấy lại tiền bị trao, thu hồi tiền lừa đảo,… với cam kết chỉ thu tiền sau khi người dân đã lấy lại được tiền bị lừa đảo. Khi có người liên hệ, đối tượng cam kết hỗ trợ việc lấy lại tiền bị lừa đảo với thủ tục nhanh chóng, đơn giản, hướng dẫn bị hại cung cấp thông tin cá nhân, tài khoản ngân hàng, số tiền bị lừa,… Căn cứ vào số tiền người dân cung cấp, các đối tượng yêu cầu phải đóng các loại phí, hoặc làm nhiệm vụ để lấy lại tiền. Khi người dân chuyển tiền, chúng thông báo tài khoản ngân hàng bị lỗi và không cho rút tiền về. Thậm chí, kẻ lừa đảo còn dụ dỗ bị hại đi cùng sang các nước lân cận Việt Nam liên hệ lấy lại tiền nhưng mục đích là bán bị hại cho các ổ, nhóm tội phạm.

Khuyến cáo: người dân không nghe theo, liên hệ với các website, fanpage, tài khoản mạng xã hội quảng cáo dịch vụ tiếp nhận hồ sơ, hỗ trợ lấy lại tiền bị treo, thu hồi tiền lừa đảo,… trên không gian mạng. Không chuyển tiền cho các đối tượng trên để được "hướng dẫn, hoàn thiện hồ sơ". Lực lượng An ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao không phối hợp, ủy quyền cho bất cứ đơn vị nào để hướng dẫn, nhận hồ sơ của người dân về các vụ lừa đảo, chiếm đoạt tài sản qua mạng; không bao giờ yêu cầu người dân đóng bất kỳ loại phí hoặc làm nhiệm vụ để tiếp nhận hồ sơ, lấy lại tiền.