ĐỀ CƯƠNG TUYÊN TRUYỀN

Về bảo đảm an ninh mạng, bảo mật thông tin, an toàn dữ liệu

(Ban hành kèm theo Công văn số -CV/BTGDVTU, ngày /11/2025 của Ban Tuyên giáo và Dân vận Tỉnh ủy)

An ninh mạng, bảo mật thông tin và an toàn dữ liệu đang trở thành những vấn đề cấp thiết, ảnh hưởng trực tiếp đến cá nhân, tổ chức và an ninh quốc gia. Với sự phát triển nhanh chóng của công nghệ thông tin và không gian mạng, các mối đe dọa từ tội phạm mạng, gián điệp mạng và khủng bố mạng ngày càng tinh vi, phức tạp. Tài liệu này được biên soạn nhằm cung cấp những kiến thức cơ bản, dễ hiểu, dễ nhớ về tình hình an ninh mạng, các nguy cơ tiềm ẩn và những biện pháp phòng ngừa, bảo vệ thiết thực, giúp mỗi cá nhân và tổ chức nâng cao ý thức, trách nhiệm, cùng nhau xây dựng một không gian mạng an toàn, lành mạnh.

I. TÌNH HÌNH CHUNG VỀ AN NINH MẠNG

1. Tình hình An ninh mạng Quốc gia

Việt Nam là một trong những quốc gia có tỷ lệ người dùng internet cao trên thế giới, với khoảng 78,44 triệu người *(chiếm gần 79,1% dân số)* và hơn 168,5 triệu thuê bao di động vào năm 2024. Việt Nam xếp hạng 16 về chỉ số an toàn, an ninh mạng toàn cầu theo Báo cáo của Liên minh Viễn thông quốc tế ITU. Tuy nhiên, Việt Nam cũng nằm trong nhóm các quốc gia bị tấn công mạng nhiều nhất tại khu vực châu Á - Thái Bình Dương .

Tính riêng trong năm 2024, tình hình tấn công mạng tại Việt Nam diễn biến phức tạp và có xu hướng gia tăng đáng báo động. Các cơ quan chức năng đã phát hiện 83 chiến dịch tấn công mạng từ 45 nhóm tin tặc, gián điệp mạng quốc tế, nhắm vào các hệ thống thông tin trọng yếu của nhiều cơ quan nhà nước và doanh nghiệp lớn. Các cuộc tấn công mã hóa dữ liệu đòi tiền chuộc quy mô lớn chưa từng có đã gây thiệt hại nghiêm trọng về kinh tế và ảnh hưởng đến an ninh trật tự xã hội. Phát hiện và xử lý hơn 70 vụ rò rỉ, phát tán tài liệu bí mật nhà nước trên mạng *(tăng gấp đôi năm 2023)* với 222 đầu tài liệu, hàng trăm GB dữ liệu nhạy cảm bị lộ. Đồng thời, phát hiện hơn 9.600 trang, blog, tài khoản mạng xã hội đăng tải gần 34.000 nội dung xấu độc, chống phá Đảng, Nhà nước, kích động gây rối an ninh, trật tự. Tuy nhiên, các cơ quan chức năng đã tăng cường kiểm soát chặt chẽ, kịp thời ngăn chặn, xử lý hiệu quả thông tin xấu độc, góp phần giữ vững ổn định xã hội.

2. Tình hình An ninh mạng tại Lạng Sơn

Tình hình an ninh mạng tại Lạng Sơn cơ bản được kiểm soát, góp phần ổn định an ninh trật tự, nhưng vẫn tiềm ẩn nguy cơ cao bị tấn công mạng, đánh cắp dữ liệu, lộ bí mật nhà nước. Đáng chú ý, tại một số cơ quan vẫn xảy ra tình trạng mất an toàn thông tin mạng do chủ quan, cài đặt mật khẩu đơn giản, hoặc kết nối thiết bị ngoại vi không an toàn.

Công an tỉnh đã kịp thời phối hợp với các cơ quan, đơn vị chức năng ngăn chặn, xử lý 07 vụ việc có dấu hiệu mất an ninh mạng, lộ văn bản nội bộ, bí mật nhà nước.

Các hoạt động tuyên truyền, chống phá Đảng và Nhà nước trên không gian mạng tại Lạng Sơn cơ bản được kiểm soát. Tuy nhiên, vào các thời điểm nhạy cảm chính trị, các đối tượng phản động lưu vong, đối tượng cực đoan lợi dụng đăng tải thông tin xuyên tạc, sai sự thật về lãnh đạo tỉnh và lực lượng công an. Cụ thể, đã phát hiện 15 tài khoản mạng xã hội của đối tượng phản động ở nước ngoài, 09 Fanpage, 08 nhóm Facebook, 04 nhóm kín Zalo và 114 tài khoản cá nhân đăng tải nội dung xấu độc, gây dư luận trái chiều, ảnh hưởng đến an ninh trật tự.

Hoạt động của các hội, nhóm và các cá nhân có ảnh hưởng (KOLs) trên địa bàn cơ bản được kiểm soát. Đã có 26 trường hợp KOLs hoạt động tích cực, quảng bá hình ảnh Lạng Sơn. Mặc dù chưa phát hiện hội nhóm chống đối liên quan an ninh quốc gia, trật tự an toàn xã hội, nhưng vẫn tồn tại một số KOLs và nhóm Facebook đăng tải thông tin phức tạp, nhạy cảm, thu hút nhiều bình luận tiêu cực. Lực lượng Công an đã chỉ đạo quản lý, chấn chỉnh 02 KOLs, vận động 02 *"KOL ẩn" (quản trị viên của 02 Fanpage với hơn 300.000 thành viên)* gỡ bỏ 48 bài viết tiêu cực, nhạy cảm.

Ngoài ra, lực lượng Công an đã: Gọi hỏi, răn đe 75 trường hợp đăng tải, chia sẻ bình luận thông tin sai sự thật, tiêu cực, xúc phạm danh dự, yêu cầu gỡ bỏ và cam kết không tái phạm. Xử phạt vi phạm hành chính 23 vụ, 29 trường hợp với tổng số tiền 187.750.000 đồng. Tấn công, báo xấu 04 đợt đối với 06 tài khoản Facebook, 07 bài viết có nội dung xấu độc. Sử dụng các fanpage, tài khoản Facebook tích cực đăng tải, chia sẻ 7.278 tin, bài, bình luận 868 tin, bài định hướng dư luận, đấu tranh phản bác quan điểm sai trái, thù địch.

II. CÁC MỐI ĐE DỌA TRÊN KHÔNG GIAN MẠNG

Để bảo vệ bản thân và cộng đồng, chúng ta cần hiểu rõ các loại hình tấn công và đe dọa chính trên không gian mạng.

1. Tội phạm mạng

Tội phạm mạng là những hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện các hành vi vi phạm pháp luật hình sự. Có hai nhóm chính:

- *Tội phạm tấn công vào hệ thống máy tính:* Mục tiêu là các hoạt động bình thường của máy tính, mạng máy tính và cơ sở dữ liệu *(ví dụ: truy cập trái phép, tấn công từ chối dịch vụ (DDoS), phát tán virus, đánh cắp dữ liệu).*

- *Tội phạm truyền thống sử dụng công nghệ cao:* Là các hành vi phạm tội thông thường nhưng sử dụng máy tính, mạng máy tính, thiết bị điện tử làm công cụ, phương tiện *(ví dụ: lừa đảo qua mạng, trộm cắp tiền từ thẻ tín dụng, đánh bạc, buôn bán ma túy, rửa tiền, truyền bá văn hóa phẩm đồi trụy qua mạng).*

Mục đích chính của tội phạm mạng là phá hoại cơ sở dữ liệu, cơ sở hạ tầng thông tin; chiếm đoạt tài sản, gây thiệt hại kinh tế; hoặc bôi nhọ uy tín, nhân phẩm.

2. Gián điệp mạng

Gián điệp mạng là hành vi cố ý vượt qua các biện pháp bảo mật để chiếm đoạt, thu thập trái phép thông tin, tài nguyên thông tin trên mạng viễn thông, Internet, hệ thống thông tin, cơ sở dữ liệu của cơ quan, tổ chức, cá nhân.

Đặc điểm:

- Thường do các cơ quan đặc biệt nước ngoài, nhân viên tình báo mạng hoặc các nhóm gián điệp thực hiện.

- Hoạt động từ xa, không giới hạn không gian, thời gian, có tính ẩn danh cao và sử dụng công nghệ hiện đại.

- Mục đích là chiếm đoạt thông tin, tuyển lựa cơ sở gián điệp, phá hoại các hệ thống thông tin quan trọng liên quan đến an ninh quốc gia.

- Gây ra hậu quả đặc biệt nghiêm trọng đối với an ninh quốc gia.

3. Khủng bố mạng

Khủng bố mạng là hoạt động sử dụng không gian mạng để thực hiện các hành vi khủng bố, tài trợ khủng bố.

Đặc điểm và Mục đích:

- Do các cơ quan đặc biệt nước ngoài, đối tượng phản động lưu vong, tổ chức khủng bố quốc tế hoặc đối tượng cực đoan trong nước thực hiện.

- Mục đích là phá hoại cơ sở hạ tầng quan trọng qua không gian mạng; gây tiếng vang, khuếch trương thanh thế; tạo tâm lý hoang mang, gây mất ổn định xã hội; tống tiền, kiếm tiền tài trợ.

- Gây thiệt hại nghiêm trọng cho cơ sở hạ tầng an ninh quốc gia, kinh tế, tính mạng, tài sản của nhân dân, và uy tín của các cơ quan Nhà nước.

4. Một số hình thức tấn công và lừa đảo phổ biến nhằm vào người Việt Nam

Người dùng Việt Nam thường xuyên phải đối mặt với nhiều hình thức tấn công mạng và lừa đảo tinh vi, trong đó phổ biến nhất là lừa đảo trực tuyến. Lừa đảo trực tuyến là hình thức tội phạm mạng lợi dụng sự mất cảnh giác của người dùng để lừa đảo thu thập thông tin cá nhân hoặc tài chính. Các hình thức này có thể là:

- *Lừa đảo qua email/tin nhắn:* Kẻ gian gửi email hoặc tin nhắn giả mạo các tổ chức, ngân hàng, cơ quan nhà nước để lừa người dùng nhấp vào liên kết độc hại hoặc cung cấp thông tin cá nhân, tài khoản ngân hàng.

- *Tấn công lừa đảo có chủ đích:* Tấn công nhắm vào một cá nhân hoặc tổ chức cụ thể, sử dụng thông tin cá nhân thu thập được để tạo email hoặc tin nhắn giả mạo thuyết phục hơn.

- *Lừa đảo bằng cuộc gọi:* Kẻ gian gọi điện thoại giả danh cơ quan công an, tòa án, ngân hàng thông báo về các giao dịch đáng ngờ, yêu cầu chuyển tiền vào tài khoản *"bảo đảm"* để chiếm đoạt.

- *Lừa đảo qua mạng xã hội:* Giả mạo bạn bè, người thân hoặc các trang bán hàng, dịch vụ để lừa đảo vay tiền, chuyển khoản, mua hàng giả mạo, hoặc phát tán mã độc.

- *Tấn công mã độc (malware):* Phát tán virus, ransomware *(mã độc tống tiền)* qua email, đường link độc hại hoặc phần mềm giả mạo để chiếm quyền kiểm soát thiết bị, mã hóa dữ liệu và đòi tiền chuộc.

- *Giả mạo trang web:* Tạo ra các trang web giả mạo ngân hàng, sàn thương mại điện tử, cổng thanh toán để lừa người dùng nhập thông tin đăng nhập, mật khẩu.

III. MỘT SỐ NỘI DUNG CƠ BẢN CỦA LUẬT AN NINH MẠNG

Luật An ninh mạng số 24/2018/QH14 được Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam khóa XIV, kỳ họp thứ 5 thông qua ngày 12 tháng 6 năm 2018 và chính thức có hiệu lực thi hành từ ngày 01 tháng 01 năm 2019. Luật gồm 7 chương, 43 điều quy định về hoạt động bảo vệ an ninh quốc gia và bảo đảm trật tự, an toàn xã hội trên không gian mạng; trách nhiệm của cơ quan, tổ chức, cá nhân có liên quan, gồm:

- Chương I: Những quy định chung, từ Điều 1 đến Điều 9

- Chương II: Bảo vệ an ninh mạng đối với hệ thống thông tin quan trọng về an ninh quốc gia, từ Điều 10 đến Điều 15

- Chương III: Phòng ngừa, xử lý hành vi xâm phạm an ninh mạng, từ Điều 16 đến Điều 22

- Chương IV: Hoạt động bảo vệ an ninh mạng, từ Điều 23 đến Điều 29

- Chương V: Bảo đảm hoạt động bảo vệ an ninh mạng, từ Điều 30 đến Điều 35

- Chương VI: Trách nhiệm của cơ quan, tổ chức, cá nhân, từ Điều 36 đến Điều 42

- Chương VII: Điều khoản thi hành, tại Điều 43

Luật An ninh mạng quy định một số nội dung cơ bản sau:

* 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 tổ chức, cá nhân; Bảo vệ an ninh mạng là phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi xâm phạm an ninh mạng. *(Quy định tại Khoản 1, 2 Điều 2 của Luật)*

* Biện pháp bảo vệ an ninh mạng *(quy định tại Điều 5)* bao gồm: Thẩm định an ninh mạng; Đánh giá điều kiện an ninh mạng; Kiểm tra an ninh mạng; Giám sát an ninh mạng; Ứng phó, khắc phục sự cố an ninh mạng; Đấu tranh bảo vệ an ninh mạng; Sử dụng mật mã để bảo vệ thông tin mạng; Ngăn chặn, yêu cầu tạm ngừng,

ngừng cung cấp thông tin mạng; đình chỉ, tạm đình chỉ các hoạt động thiết lập, cung cấp và sử dụng mạng viễn thông, mạng internet, sản xuất và sử dụng thiết bị phát, thu phát sóng vô tuyến theo quy định của pháp luật; Thu thập dữ liệu điện tử liên quan đến hoạt động xâm phạm an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của tổ chức, cá nhân trên không gian mạng; Phong tỏa, hạn chế hoạt động của hệ thống thông tin; đình chỉ, tạm đình chỉ hoặc yêu cầu ngừng hoạt động của hệ thống thông tin, thu hồi tên miền theo quy định của pháp luật; xóa bỏ, truy cập, xóa bỏ thông tin trái pháp luật hoặc thông tin sai sự thật trên không gian mạng xâm phạm an ninh quốc gia, trật tự, an toàn xã hội;

* Lực lượng bảo vệ an ninh mạng gồm: Lực lượng chuyên trách bảo vệ an ninh mạng được bố trí tại Bộ Công an, Bộ Quốc phòng; Lực lượng bảo vệ an ninh mạng được bố trí tại Bộ, ngành, Ủy ban nhân dân cấp tỉnh, cơ quan, tổ chức quản lý trực tiếp hệ thống thông tin quan trọng về an ninh quốc gia; Tổ chức, cá nhân được huy động tham gia bảo vệ an ninh mạng.

* 6 nhóm hành vi bị cấm *(Theo quy định của Điều 8, có 6 nhóm hành vi bị nghiêm cấm)* gồm:

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

a. 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.

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.

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 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 sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho các 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 tổ chức, cá nhân khác.

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 tổ chức, cá nhân;

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;

Cố ý thay đổi, hủy bỏ hoặc làm vô hiệu hóa các 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;

Đưa lên không gian mạng những thông tin thuộc bí mật cá nhân, bí mật gia đình, đời sống riêng tư trái quy định của pháp luật;

Cố ý nghe, ghi âm trái phép các cuộc đàm thoại;

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;

Chiếm đoạt tài sản; tổ chức đánh bạc, đánh bạc qua mạng internet; trộm cắp cước viễn thông quốc tế trên nền internet; vi phạm bản quyền và sở hữu trí tuệ trên không gian mạng;

Giả mạo trang thông tin điện tử của cơ quan, tổ chức, cá nhân; làm giả, lưu hành, trộm cắp, mua bán, thu thập, trao đổi trái phép thông tin thẻ tín dụng, tài khoản ngân hàng của người khác; phát hành, cung cấp, sử dụng các phương tiện thanh toán trái phép;

Tuyên truyền, quảng cáo, mua bán hàng hóa, dịch vụ thuộc danh mục cám theo quy định của pháp luật;

Hướng dẫn người khác thực hiện hành vi vi phạm pháp luật;

Hành vi khác sử dụng không gian mạng vi phạm pháp luật về an ninh quốc gia, trật tự, an toàn xã hội.

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

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

d. Thông tin sai sự thật gây hoang mang trong nhân dân, gây thiệt hại cho các 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 tổ chức, cá nhân khác;

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

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

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

(3) Sản xuất, đưa vào sử dụng công cụ, phương tiện, phần mềm hoặc có hành vi cản trở, gây rối loạn hoạt động của mạng máy tính, mạng viễn thông; phát tán chương trình tin học gây hại cho hoạt động của mạng máy tính, mạng viễn thông, phương tiện điện tử; xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác.

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

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

Hiện nay, Bộ Công an đang chủ trì xây dựng Dự thảo Luật An ninh mạng sửa đổi năm 2025 nhằm thay thế Luật An ninh mạng 2018 và Luật An toàn thông tin mạng 2015. Dự thảo này nhằm hợp nhất và tối ưu hóa khung pháp lý, tăng cường khả năng bảo vệ dữ liệu và an ninh mạng của quốc gia.

IV. TRÁCH NHIỆM VÀ BIỆN PHÁP BẢO VỆ AN NINH MẠNG

Bảo vệ an ninh mạng không chỉ là trách nhiệm của các cơ quan nhà nước mà còn là trách nhiệm của mỗi cá nhân, tổ chức.

1. Trách nhiệm cá nhân trong việc bảo vệ an toàn không gian mạng

Mỗi cá nhân đóng vai trò quan trọng trong việc xây dựng một không gian mạng an toàn. Dù là người dùng internet bình thường hay chuyên gia công nghệ, chúng ta đều có thể trở thành nạn nhân của các cuộc tấn công mạng, đặc biệt khi sử dụng cùng một thiết bị cho công việc và cá nhân. Trách nhiệm cá nhân bao gồm:

- *Nâng cao nhận thức:* Chủ động tìm hiểu và cập nhật các thông tin, kiến thức về an ninh mạng, các mối đe dọa và cách phòng tránh.

- *Tuân thủ pháp luật:* Chấp hành nghiêm chỉnh các quy định của pháp luật về an ninh mạng, bảo vệ thông tin cá nhân và không phát tán thông tin xấu độc.

- *Thực hiện các biện pháp bảo mật cơ bản:* Đây là nền tảng để bảo vệ dữ liệu và thiết bị cá nhân.

2. Những việc cần làm để bảo vệ bản thân trên không gian mạng

Để tự bảo vệ mình khỏi các nguy cơ trên không gian mạng, mỗi người cần thực hiện các biện pháp sau:

2.1. Bảo vệ tài khoản và mật khẩu

- *Sử dụng mật khẩu mạnh và duy nhất:* Mật khẩu nên dài, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt. Tránh sử dụng thông tin cá nhân dễ đoán *(tên, ngày sinh)*. Không dùng chung một mật khẩu cho nhiều tài khoản .

- *Kích hoạt xác thực hai yếu tố:* Đây là lớp bảo vệ bổ sung cho tài khoản của bạn. Ngay cả khi kẻ gian biết mật khẩu, chúng cũng khó truy cập được nếu không có mã xác thực gửi đến điện thoại hoặc email của bạn.

- *Thay đổi mật khẩu định kỳ:* Đặc biệt với các tài khoản quan trọng như ngân hàng, email chính.

- *Sử dụng trình quản lý mật khẩu:* Giúp tạo và lưu trữ các mật khẩu mạnh, duy nhất một cách an toàn.

2.2. Bảo vệ thiết bị và dữ liệu

- *Cập nhật phần mềm thường xuyên:* Luôn cài đặt các bản cập nhật hệ điều hành, trình duyệt web và phần mềm ứng dụng ngay khi có thông báo. Các bản cập nhật này thường chứa các bản vá lỗi bảo mật quan trọng .

- *Sử dụng phần mềm diệt virus/phần mềm bảo mật uy tín:* Cài đặt và duy trì phần mềm bảo mật trên máy tính, điện thoại. Thực hiện quét định kỳ để phát hiện và loại bỏ mã độc.

- *Sao lưu dữ liệu quan trọng:* Thường xuyên sao lưu dữ liệu lên các thiết bị lưu trữ ngoài hoặc dịch vụ đám mây an toàn để phòng trường hợp thiết bị bị hỏng, bị đánh cắp hoặc bị mã độc tấn công.

- *Cẩn trọng khi sử dụng Wi-Fi công cộng:* Tránh truy cập vào các giao dịch nhạy cảm *(ngân hàng, mua sắm trực tuyến)* khi sử dụng Wi-Fi công cộng không bảo mật. Nên sử dụng Mạng riêng ảo *(VPN)* để mã hóa dữ liệu khi cần.

- *Bảo vệ thiết bị vật lý:* Luôn khóa thiết bị khi không sử dụng, cài đặt mật khẩu/mã PIN/sinh trắc học cho điện thoại, máy tính bảng. Cẩn thận khi cho người khác mượn hoặc để thiết bị không có người trông coi.

2.3. Cẩn trọng khi tương tác trực tuyến

- *Nghi ngờ các liên kết và tệp đính kèm lạ:* Tuyệt đối không nhấp vào các liên kết đáng ngờ hoặc mở các tệp đính kèm từ email/tin nhắn không rõ nguồn gốc. Đây là con đường phổ biến nhất để phát tán mã độc và lừa đảo.

- *Xác minh thông tin trước khi hành động:* Khi nhận được yêu cầu cung cấp thông tin cá nhân, chuyển tiền hoặc cài đặt ứng dụng từ các thông báo khẩn cấp, hãy xác minh trực tiếp với tổ chức/cá nhân đó qua kênh liên lạc chính thức *(không dùng số điện thoại/email trong tin nhắn đáng ngờ).*

- *Cẩn trọng với thông tin cá nhân trên mạng xã hội:* Hạn chế chia sẻ thông tin nhạy cảm *(địa chỉ, số điện thoại, thông tin gia đình)* công khai. Điều chỉnh cài đặt riêng tư của các tài khoản mạng xã hội.

- *Kiểm tra địa chỉ trang web:* Luôn đảm bảo địa chỉ trang web bắt đầu bằng "https://" và có biểu tượng ổ khóa trước khi nhập thông tin cá nhân hoặc thực hiện giao dịch.

- *Tránh tham gia các hội nhóm có nội dung xấu độc:* Không truy cập, chia sẻ, bình luận các thông tin xuyên tạc, bịa đặt, kích động trên không gian mạng.

V. LIÊN HỆ KHI GẶP SỰ CỐ AN NINH MẠNG

Khi gặp phải các tình huống liên quan đến an ninh mạng như bị lừa đảo, mất tài khoản, hoặc nghi ngờ thiết bị bị nhiễm mã độc, cần phải hành động nhanh chóng và liên hệ với các cơ quan chức năng để được hỗ trợ kịp thời.

1. Các kênh liên hệ và hỗ trợ:

- *Cơ quan Công an địa phương:* Nếu bạn là nạn nhân của lừa đảo chiếm đoạt tài sản, bị lộ lọt thông tin cá nhân nghiêm trọng, hoặc phát hiện các hành vi vi phạm pháp luật trên không gian mạng, hãy đến trình báo tại cơ quan công an gần nhất để được hướng dẫn và xử lý.

- *Ngân hàng hoặc Tổ chức tài chính:* Nếu giao dịch ngân hàng của bạn bị xâm phạm, thẻ tín dụng bị lợi dụng, hãy liên hệ ngay với ngân hàng phát hành thẻ hoặc tổ chức tài chính liên quan để khóa tài khoản, thẻ và được hỗ trợ xử lý.

- *Nhà cung cấp dịch vụ Internet (ISP) hoặc nhà mạng di động:* Nếu bạn gặp vấn đề về kết nối, truy cập các trang web độc hại hoặc nhận các tin nhắn lừa đảo qua mạng viễn thông, hãy liên hệ với nhà cung cấp dịch vụ của mình để được hỗ trợ kỹ thuật và chặn các nguồn gây hại.

- *Nền tảng mạng xã hội/Dịch vụ trực tuyến:* Nếu tài khoản mạng xã hội, email hoặc tài khoản dịch vụ trực tuyến của bạn bị hack, hãy sử dụng tính năng hỗ trợ, báo cáo của chính nền tảng đó để khôi phục tài khoản và báo cáo hành vi vi phạm.

2. Lưu ý quan trọng:

- *Giữ bình tĩnh:* Khi phát hiện sự cố, điều quan trọng là phải giữ bình tĩnh để có thể đưa ra quyết định đúng đắn.

- *Thu thập bằng chứng:* Ghi lại mọi thông tin liên quan đến sự cố *(tin nhắn lừa đảo, email, ảnh chụp màn hình các giao dịch đáng ngờ, địa chỉ trang web giả mạo...)* để cung cấp cho cơ quan chức năng.

- *Không tự ý xử lý nếu không có chuyên môn:* Tránh tự ý can thiệp vào các vấn đề kỹ thuật phức tạp nếu bạn không có kiến thức chuyên môn, điều này có thể làm mất bằng chứng hoặc làm tình hình tồi tệ hơn.

***

An ninh mạng là một cuộc chiến không ngừng nghỉ, đòi hỏi sự chung tay của toàn xã hội. Từ những thách thức và nguy cơ hiện hữu trên không gian mạng quốc gia và tại Lạng Sơn, có thể thấy rõ tầm quan trọng của việc nâng cao ý thức và trang bị kiến thức bảo mật cho mọi đối tượng. Mỗi cá nhân, tổ chức cần chủ động tìm hiểu, nắm vững các quy định pháp luật, đồng thời thực hành các biện pháp bảo vệ thông tin, dữ liệu cá nhân một cách nghiêm túc. Qua đó, góp phần xây dựng một môi trường mạng an toàn, lành mạnh hơn, biến không gian mạng thành một công cụ hữu ích, phục vụ sự phát triển.