Bo v bí mt nhà nc trên không gian mng: Chuyên dùng cho ào to trình i hc CSND, h Chính quy theo tin ch - Lu hành ni b

inh Vit Hùng; H Nguyn Xuân Thanh

2025
Trng i hc CSND
https://library.dhcsnd.edu.vn/handle/123456789/72

BỘ CÔNG AN
TRƯỜNG ĐẠI HỌC CẢNH SÁT NHÂN DÂN

CHUYÊN ĐỀ

BẢO VỆ BÍ MẬT NHÀ NƯỚC TRÊN KHÔNG GIAN MẠNG

(Dùng cho đào tạo trình độ Đại học CSND)
Ban hành kèm theo Quyết định số …ngày …tháng… năm …của…

LƯU HÀNH NỘI BỘ

TP. HỒ CHÍ MINH – 2025

BAN BIÊN SOẠN CHUYÊN ĐỀ

Chủ biên: Thạc sĩ Đinh Việt Hùng, Giảng viên, Khoa Ngoại Ngữ Tin học

Tham gia biên soạn:

1. ThS Đinh Việt Hùng, Giảng viên, Khoa NN-TH, *Chương 1, 2.*
2. ThS Hồ Nguyễn Xuân Thanh, Giảng viên, Khoa NN-TH, *Chương 3.*

Mẫu số 2.2 – X02

HỘI ĐỒNG THẨM ĐỊNH CHUYÊN ĐỀ

(Thành lập theo Quyết định số QĐ-T05, ngày tháng năm 2025 của Hiệu trưởng Trường Đại học CSND)

STT	Họ tên (Ghi rõ cấp bậc, học hàm, học vị, chức danh công tác)	Chức vụ	Đơn vị công tác	Chức danh trong hội đồng thẩm định
1.	PGS.TS Nguyễn Giang Nam	Phó Hiệu trưởng	T05	Chủ tịch
2.	ThS Nguyễn Thanh Trung	Trưởng Phòng	T05	UV phản biện 1
3.	ThS Tạ Đức	Giám đốc TT	T05	UV phản biện 2
4.	ThS Nguyễn Thị Mai Thanh	Cán bộ	T05	Thư ký
5.	PGS. TS Bùi Ngọc Hà	Trưởng phòng	T05	Ủy viên
6.	TS Võ Thành Đạt	Trưởng khoa	T05	Ủy viên
7.	ThS Trần Quang Phúc	Cán bộ	T05	Ủy viên
Thư ký hành chính: ThS Nguyễn Thị Mai Thanh Cán bộ phòng QLNCKH				

LỜI NÓI ĐẦU

Trong thời đại công nghệ số phát triển mạnh mẽ, mạng Internet đã trở thành một phần không thể tách rời của đời sống xã hội, đóng vai trò quan trọng trong mọi lĩnh vực từ kinh tế, chính trị, văn hóa đến an ninh quốc phòng. Tuy nhiên, cùng với những lợi ích to lớn, không gian mạng cũng tiềm ẩn nhiều nguy cơ, thách thức, đặc biệt là nguy cơ lộ, lọt, mất bí mật Nhà nước (BMNN).

Việc bảo vệ BMNN trên không gian mạng không chỉ là trách nhiệm của các cơ quan, tổ chức mà còn là nghĩa vụ của mỗi cá nhân. Những hành vi bất cẩn, thiếu hiểu biết hoặc cố ý vi phạm có thể gây hậu quả nghiêm trọng, ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội. Chính vì vậy, việc nâng cao nhận thức, hiểu biết pháp luật và trang bị các kỹ năng bảo vệ thông tin trên không gian mạng là vô cùng cần thiết.

Chuyên đề **"Bảo vệ bí mật Nhà nước trên không gian mạng"** nhằm cung cấp những kiến thức cơ bản về BMNN, các nguy cơ mất an toàn thông tin trên không gian mạng, cũng như các biện pháp phòng ngừa, xử lý khi BMNN bị lộ, lọt, bị mất. Qua đó, giúp mỗi cá nhân, tổ chức nâng cao ý thức và trách nhiệm trong việc giữ gìn, bảo vệ thông tin quan trọng, góp phần bảo đảm an ninh, chủ quyền quốc gia trong thời đại kỷ nguyên số.

Nội dung chuyên đề bao gồm:

Chương 1: Tổng quan về BMNN và Không gian mạng

Chương 2: Những nguy cơ và thách thức trong bảo vệ BMNN trên không gian mạng

Chương 3: Kỹ năng phòng, chống lộ, mất BMNN trên không gian mạng

Chuyên đề được biên soạn theo hướng thực tiễn, gắn liền với nhiệm vụ công tác của cán bộ CAND. Nội dung tài liệu được trình bày ngắn gọn, dễ hiểu, có nhiều số liệu thực tế, giúp người đọc dễ dàng nắm bắt kiến thức và vận dụng vào thực tiễn công tác.

Ban biên soạn xin trân thành cảm ơn đóng góp của quý thầy, cô trong Khoa Ngoại ngữ - Tin học và một số chuyên gia trong, ngoài trường đã có những góp ý và đánh giá một số nội dung giúp nhóm tác giả hoàn thành được chuyên đề.

TRƯỜNG ĐẠI HỌC CSND

CHƯƠNG 1. TỔNG QUAN VỀ BÍ MẬT NHÀ NƯỚC VÀ KHÔNG GIAN MẠNG

I. BÍ MẬT NHÀ NƯỚC VÀ CÁC QUY ĐỊNH CỦA PHÁP LUẬT LIÊN QUAN

1. Một số khái niệm

a. Bí mật Nhà nước

Theo Luật bảo vệ bí mật Nhà nước (BMNN) năm 2018 (Luật số 29/2018/QH14) do Quốc hội nước Cộng hòa xã hội chủ nghĩa Việt Nam ban hành, "*BMNN là thông tin có nội dung quan trọng do người đứng đầu cơ quan, tổ chức có thẩm quyền xác định căn cứ vào quy định của Luật này, chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc*".

Hình thức chứa BMNN bao gồm tài liệu, vật, địa điểm, lời nói, hoạt động hoặc các dạng khác có nội dung quan trọng liên quan đến chính trị, quốc phòng, an ninh, đối ngoại, kinh tế, khoa học, công nghệ và các lĩnh vực khác.

Theo Luật này, căn cứ vào tính chất quan trọng của nội dung thông tin, mức độ nguy hại nếu bị lộ, bị mất, BMNN được xác định theo 3 cấp độ:

Mật: là BMNN liên quan đến chính trị, quốc phòng, an ninh, cơ yếu, lập hiến, lập pháp, tư pháp, đối ngoại, kinh tế, tài nguyên và môi trường, khoa học và công nghệ, giáo dục và đào tạo, văn hóa, thể thao, thông tin và truyền thông, y tế, dân số, lao động, xã hội, tổ chức, cán bộ, thanh tra, kiểm tra, giám sát, xử lý vi phạm, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng, kiểm toán nhà nước, nếu bị lộ, lọt có thể gây nguy hại nghiêm trọng đến lợi ích quốc gia, dân tộc.

Tuyệt mật: là BMNN liên quan đến chính trị, quốc phòng, an ninh, cơ yếu, đối ngoại, nếu bị lộ, lọt có thể gây nguy hại đặc biệt nghiêm trọng đến lợi ích quốc gia, dân tộc.

Tối mật: là BMNN liên quan đến chính trị, quốc phòng, an ninh, cơ yếu, lập hiến, lập pháp, tư pháp, đối ngoại, kinh tế, tài nguyên và môi trường, khoa học và công nghệ, giáo dục và đào tạo, văn hóa, thể thao, thông tin và truyền thông, y tế, dân số, lao động, xã hội, tổ chức, cán bộ, thanh tra, kiểm tra, giám sát, xử lý vi phạm, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng, kiểm toán nhà nước, nếu bị lộ, lọt có thể gây nguy hại rất nghiêm trọng đến lợi ích quốc gia, dân tộc.

b. Bảo vệ bí mật Nhà nước

Là việc cơ quan, tổ chức, cá nhân sử dụng lực lượng, phương tiện, biện pháp để phòng, chống xâm phạm BMNN, ngăn chặn việc lộ, lọt, thu thập, sử dụng trái

phép thông tin thuộc danh mục BMNN, đảm bảo an toàn cho các thông tin quan trọng liên quan đến lợi ích quốc gia, dân tộc.

Các hành vi bị cấm trong bảo vệ BMNN theo Điều 5 Luật bảo vệ BMNN năm 2018 gồm:

- Làm lộ, chiếm đoạt, mua, bán BMNN; làm sai lệch, hư hỏng, mất tài liệu, vật chứa BMNN.

- Thu thập, trao đổi, cung cấp, chuyển giao BMNN trái pháp luật; sao, chụp, lưu giữ, vận chuyển, giao, nhận, thu hồi, tiêu hủy tài liệu, vật chứa BMNN trái pháp luật.

- Mang tài liệu, vật chứa BMNN ra khỏi nơi lưu giữ trái pháp luật.

- Lợi dụng, lạm dụng việc bảo vệ BMNN, sử dụng BMNN để thực hiện, che giấu hành vi vi phạm pháp luật, xâm phạm quyền và lợi ích hợp pháp hoặc cản trở hoạt động của cơ quan, tổ chức, cá nhân.

- Soạn thảo, lưu giữ tài liệu có chứa nội dung BMNN trên máy tính hoặc thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ BMNN theo quy định của pháp luật về cơ yếu.

- Truyền đưa BMNN trên phương tiện thông tin, viễn thông trái với quy định của pháp luật về cơ yếu.

- Chuyển mục đích sử dụng máy tính, thiết bị khác đã dùng để soạn thảo, lưu giữ, trao đổi BMNN khi chưa loại bỏ BMNN.

- Sử dụng thiết bị có tính năng thu, phát tín hiệu, ghi âm, ghi hình trong hội nghị, hội thảo, cuộc họp có nội dung BMNN dưới mọi hình thức khi chưa được người có thẩm quyền cho phép.

- Đăng tải, phát tán BMNN trên phương tiện thông tin đại chúng, mạng Internet, mạng máy tính và mạng viễn thông.

c. Lộ bí mật Nhà nước

Là trường hợp thông tin thuộc danh mục BMNN bị người không có trách nhiệm biết được, gây nguy cơ ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội hoặc các lợi ích quan trọng của đất nước.

Đây là một trong những nguy cơ nghiêm trọng trong công tác bảo vệ BMNN, đặc biệt trong bối cảnh không gian mạng phát triển mạnh mẽ, làm gia tăng rủi ro rò rỉ thông tin.

d. Mất bí mật Nhà nước

Là trường hợp tài liệu, vật chứa BMNN không còn thuộc sự quản lý của cơ quan, tổ chức, cá nhân có trách nhiệm quản lý, dẫn đến nguy cơ bị lộ, lọt thông tin quan trọng, ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội và lợi ích dân tộc; làm suy giảm uy tín, an toàn hoạt động của cơ quan, tổ chức liên quan.

2. Nguyên tắc bảo vệ BMNN

Bảo vệ BMNN phải tuân thủ các nguyên tắc đảm bảo việc quản lý, sử dụng và bảo vệ BMNN được thực hiện một cách chặt chẽ, đúng quy định pháp luật, góp phần giữ vững an ninh quốc gia và trật tự an toàn xã hội.

Nguyên tắc 1: Đặt dưới sự lãnh đạo của Đảng Cộng sản Việt Nam, sự quản lý thống nhất của Nhà nước; phục vụ nhiệm vụ xây dựng và bảo vệ Tổ quốc, phát triển kinh tế - xã hội, hội nhập quốc tế của đất nước; bảo vệ lợi ích quốc gia, dân tộc, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân.

Nguyên tắc 2: Bảo vệ BMNN là trách nhiệm của mọi cơ quan, tổ chức, cá nhân.

Nguyên tắc 3: Việc quản lý, sử dụng BMNN bảo đảm đúng mục đích, thẩm quyền, trình tự, thủ tục theo quy định của pháp luật.

Nguyên tắc 4: Chủ động phòng ngừa; kịp thời phát hiện, ngăn chặn, xử lý nghiêm hành vi vi phạm pháp luật về bảo vệ BMNN.

Nguyên tắc 5: BMNN được bảo vệ theo thời hạn quy định của Luật này, bảo đảm quyền tiếp cận thông tin của công dân theo quy định của pháp luật.

3. Phạm vi bí mật Nhà nước

Phạm vi BMNN là giới hạn thông tin quan trọng trong các lĩnh vực sau đây chưa được công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc:

a. Thông tin về chính trị:

Chủ trương, chính sách của Đảng và Nhà nước về đối nội, đối ngoại; - Hoạt động của Ban Chấp hành Trung ương, Bộ Chính trị, Ban Bí thư và lãnh đạo Đảng, Nhà nước;

Chiến lược, đề án về dân tộc, tôn giáo và công tác dân tộc, tôn giáo liên quan đến bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội;

Thông tin có tác động tiêu cực đến tình hình chính trị, kinh tế - xã hội.

b. Thông tin về quốc phòng, an ninh, cơ yếu:

Chiến lược, kế hoạch, phương án, hoạt động bảo vệ Tổ quốc, phòng thủ đất nước, bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; chương trình, dự án, đề án đặc biệt quan trọng;

Tổ chức và hoạt động của lực lượng vũ trang nhân dân, lực lượng cơ yếu;

Công trình, mục tiêu về quốc phòng, an ninh, cơ yếu; các loại vũ khí, khí tài, phương tiện quyết định khả năng phòng thủ đất nước, bảo vệ an ninh quốc gia, bảo đảm trật tự, an toàn xã hội; sản phẩm mật mã của cơ yếu.

c. Thông tin về lập hiến, lập pháp, tư pháp:

Hoạt động lập hiến, lập pháp, giám sát, quyết định vấn đề quan trọng của đất nước;

Thông tin về khởi tố; công tác điều tra, thực hành quyền công tố, kiểm sát hoạt động tư pháp, xét xử, thi hành án hình sự.

d. Thông tin về đối ngoại:

Chiến lược, kế hoạch, đề án phát triển quan hệ với nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế; tình hình, phương án, kế hoạch, hoạt động đối ngoại của cơ quan Đảng, Nhà nước;

Thông tin, thỏa thuận được trao đổi, ký kết giữa Việt Nam với nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế;

Thông tin bí mật do nước ngoài, tổ chức quốc tế hoặc chủ thể khác của pháp luật quốc tế chuyển giao theo điều ước quốc tế mà nước Cộng hòa xã hội chủ nghĩa Việt Nam là thành viên và thỏa thuận quốc tế có liên quan.

e. Thông tin về kinh tế:

Chiến lược, kế hoạch đầu tư và dự trữ quốc gia bảo đảm quốc phòng, an ninh; đấu thầu phục vụ bảo vệ an ninh quốc gia;

Thông tin về tài chính, ngân sách, ngân hàng; phương án, kế hoạch thu, đổi, phát hành tiền; thiết kế mẫu, chế tạo bản in, khuôn đúc, công nghệ in, đúc tiền và giấy tờ có giá; số lượng, nơi lưu giữ kim loại quý hiếm, đá quý và vật quý hiếm khác của Nhà nước;

Thông tin về công nghiệp, thương mại, nông nghiệp và phát triển nông thôn;

Kế hoạch vận tải có ý nghĩa quan trọng về chính trị, kinh tế - xã hội, quốc phòng, an ninh;

Thông tin về quá trình xây dựng quy hoạch cấp quốc gia, quy hoạch vùng,

quy hoạch tỉnh, quy hoạch đơn vị hành chính - kinh tế đặc biệt, quy hoạch đô thị, quy hoạch nông thôn; thông tin về quy hoạch hệ thống kho dự trữ quốc gia, quy hoạch hệ thống các công trình quốc phòng, khu quân sự, kho đạn dược, công nghiệp quốc phòng, an ninh.

f. Thông tin về tài nguyên và môi trường bao gồm tài nguyên nước, môi trường, địa chất, khoáng sản, khí tượng thủy văn, đất đai, biển, hải đảo, đo đạc và bản đồ.

g. Thông tin về khoa học và công nghệ:

Sáng chế, công nghệ mới phục vụ quốc phòng, an ninh hoặc có ý nghĩa đặc biệt quan trọng đối với phát triển kinh tế - xã hội;

Thông tin về năng lượng nguyên tử, an toàn bức xạ và hạt nhân liên quan đến quốc phòng, an ninh;

Nhiệm vụ khoa học và công nghệ đặc biệt, nhiệm vụ khoa học và công nghệ cấp quốc gia liên quan đến quốc phòng, an ninh.

h. Thông tin về giáo dục và đào tạo:

Đề thi, đáp án và thông tin liên quan đến việc tổ chức kỳ thi cấp quốc gia;

Thông tin về người thuộc Quân đội nhân dân, Công an nhân dân, Cơ yếu được cử đi đào tạo trong nước và ngoài nước.

i. Thông tin về văn hóa, thể thao:

Thông tin về di sản, di vật, cổ vật, bảo vật quốc gia; phương pháp, bí quyết sáng tạo, giữ gìn, trao truyền di sản văn hóa phi vật thể;

Phương pháp, bí quyết tuyển chọn huấn luyện viên, vận động viên các môn thể thao thành tích cao; biện pháp, bí quyết phục hồi sức khỏe vận động viên sau tập luyện, thi đấu; đấu pháp trong thi đấu thể thao thành tích cao.

j. Lĩnh vực thông tin và truyền thông:

Chiến lược, kế hoạch, đề án phát triển báo chí, xuất bản, in, phát hành, bưu chính, viễn thông và Internet, tần số vô tuyến điện, công nghệ thông tin, công nghiệp công nghệ thông tin, an toàn thông tin mạng, điện tử, phát thanh và truyền hình, thông tin điện tử, thông tấn, thông tin đối ngoại, thông tin cơ sở và hạ tầng thông tin và truyền thông quốc gia để phục vụ quốc phòng, an ninh;

Thiết kế kỹ thuật, sơ đồ, số liệu về thiết bị của hệ thống thông tin quan trọng về an ninh quốc gia, hệ thống thông tin quan trọng quốc gia và hệ thống mạng thông tin dùng riêng phục vụ cơ quan, tổ chức của Đảng, Nhà nước.

k. Thông tin về y tế, dân số:

Thông tin bảo vệ sức khỏe lãnh đạo cấp cao của Đảng, Nhà nước;

Chủng, giống vi sinh vật mới phát hiện liên quan đến sức khỏe, tính mạng con người; mẫu vật, nguồn gen, vùng nuôi trồng dược liệu quý hiếm;

Quy trình sản xuất dược liệu, thuốc sinh học quý hiếm;

Thông tin, tài liệu, số liệu điều tra về dân số.

l. Thông tin về lao động, xã hội:

Chiến lược, kế hoạch, đề án về cải cách tiền lương, bảo hiểm xã hội, người có công với cách mạng;

Tình hình phức tạp về lao động, trẻ em, tệ nạn xã hội, bình đẳng giới.

m. Thông tin về tổ chức, cán bộ:

Chiến lược, kế hoạch, đề án về công tác tổ chức, cán bộ của cơ quan Đảng, Nhà nước, tổ chức chính trị - xã hội;

Quy trình chuẩn bị và triển khai, thực hiện công tác tổ chức, cán bộ;

Thông tin về công tác bảo vệ chính trị nội bộ;

Đề thi, đáp án thi tuyển chọn lãnh đạo, quản lý và tuyển dụng, nâng ngạch công chức, viên chức.

n. Thông tin về thanh tra, kiểm tra, giám sát, xử lý vi phạm, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng:

Chiến lược, kế hoạch, đề án về công tác thanh tra, kiểm tra, giám sát, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng;

Thông tin về hoạt động thanh tra, kiểm tra, giám sát, xử lý vi phạm, giải quyết khiếu nại, tố cáo và phòng, chống tham nhũng.

o. Thông tin về kiểm toán nhà nước:

Chiến lược, kế hoạch, đề án về kiểm toán nhà nước;

Thông tin kiểm toán về tài chính công, tài sản công.

4. Tầm quan trọng của việc bảo vệ BMNN trong bối cảnh hiện nay

BMNN đóng vai trò then chốt trong việc bảo vệ chủ quyền quốc gia, đảm bảo an ninh và trật tự điều hành đất nước. Dưới áp lực từ các thế lực thù địch, gián điệp và tin tặc, BMNN trở thành mục tiêu hàng đầu cần được quan tâm đặc biệt. Các quốc gia lớn trên thế giới đã và đang tăng cường bảo vệ BMNN trên không

gian mạng bằng nhiều biện pháp kỹ thuật và pháp lý.

Tình trạng lộ BMNN trên không gian mạng đang là một vấn đề đáng báo động. Các đối tượng xấu thường sử dụng các thủ đoạn tinh vi để xâm nhập, đánh cắp, mua bán, trao đổi BMNN trên mạng internet, gây ra những hậu quả nghiêm trọng cho quốc gia. Sự phát triển công nghệ thông tin, Internet và trí tuệ nhân tạo đã mở ra những cơ hội lớn, nhưng đồng thời cũng đặt ra thách thức về an ninh thông tin quốc gia. Việc lộ, rò rỉ hoặc mất BMNN không chỉ ảnh hưởng đến an ninh quốc gia mà còn gây nguy hại cho sự ổn định chính trị, kinh tế và xã hội. Cụ thể là:

Đe dọa an ninh quốc gia: BMNN bị lộ có thể đặt an ninh quốc gia vào tình trạng nguy hiểm, tạo cơ hội cho các lực lượng thù địch khai thác thông tin để thực hiện các hoạt động gián điệp, phá hoại hoặc kích động bất ổn chính trị. Điều này có thể dẫn đến các chiến dịch truyền thông bôi nhọ, tấn công mạng nhằm làm suy yếu niềm tin của người dân vào Đảng, Nhà nước và chính quyền, thậm chí gây ra các xung đột tiềm ẩn làm mất ổn định đất nước.

Tác động nghiêm trọng đến kinh tế: Những thông tin về chính sách tài chính, đầu tư, quy hoạch phát triển bị lộ có thể gây biến động trên thị trường, làm suy giảm niềm tin của nhà đầu tư, dẫn đến rút vốn ồ ạt, sụt giảm giá trị tiền tệ và chứng khoán. Các doanh nghiệp có thể đối mặt với tình trạng cạnh tranh không lành mạnh do đối thủ nắm được thông tin chiến lược, làm suy yếu khả năng phát triển của nền kinh tế trong dài hạn. Đồng thời, việc lộ thông tin có thể tạo điều kiện cho các tổ chức tài chính quốc tế đánh giá thấp mức độ ổn định của nền kinh tế, ảnh hưởng tiêu cực đến xếp hạng tín nhiệm quốc gia.

Gây bất ổn xã hội: Thông tin "nhạy cảm" bị rò rỉ rất dễ bị kẻ xấu lợi dụng để xuyên tạc, kích động biểu tình, gây mất đoàn kết trong cộng đồng. Các thế lực thù địch có thể sử dụng những thông tin này để thao túng dư luận, lan truyền tin giả nhằm gây hoang mang trong nhân dân, làm mất lòng tin vào chính quyền. Điều này có thể dẫn đến rối loạn trật tự công cộng, ảnh hưởng đến an ninh chính trị, thậm chí gây ra các cuộc khủng hoảng xã hội hoặc tiến tới "*cách mạng màu*" nếu không được kiểm soát kịp thời.

Gây thất thoát và thiệt hại trong quốc phòng: BMNN bị rò rỉ về quốc phòng có thể giúp kẻ thù thu thập thông tin về sức mạnh quân đội, bao gồm chiến lược tác chiến, bố trí lực lượng, vũ khí trang bị và kế hoạch phòng thủ. Điều này làm tăng nguy cơ bị tấn công bất ngờ, mất lợi thế chiến lược và bị đối phương thao túng trong các vấn đề an ninh khu vực. Ngoài ra, thông tin mật về công nghệ quốc phòng

bị lộ có thể bị sao chép, làm suy giảm năng lực cạnh tranh quân sự, ảnh hưởng nghiêm trọng đến khả năng phòng thủ và bảo vệ chủ quyền quốc gia.

5. Các quy định về bảo vệ BMNN trên không gian mạng

a. Nhóm các văn bản quy định về bảo vệ BMNN

Luật Bảo vệ BMNN; Nghị định 26/2020/NĐ-CP ngày 28/2/2020 của Chính phủ quy định chi tiết một số điều của Luật Bảo vệ BMNN; Thông tư 104/2021/TT-BCA ngày 08/11/2021 của Bộ Công an quy định về công tác bảo vệ BMNN trong Công an nhân dân; Chỉ thị số 05/2012/CT-TTg, ngày 21/02/2012 của Thủ tướng Chính phủ về nâng cao chất lượng, hiệu quả công tác bảo vệ BMNN trong tình hình mới; Chỉ thị số 02/CT-BCA ngày 27/4/2021 của Bộ Công an về tăng cường công tác phòng, chống tấn công mạng và bảo vệ BMNN trên không gian mạng trong Công an nhân dân…

Liên quan đến bảo vệ BMNN trên không gian mạng, Điều 5, Luật Bảo vệ BMNN nêu rõ các hành vi bị nghiêm cấm:

"…Thu thập, trao đổi, cung cấp, chuyển giao BMNN trái pháp luật; sao, chụp, lưu trữ, vận chuyển, giao, nhận, thu hồi, tiêu hủy tài liệu, vật chứa BMNN trái pháp luật

- Soạn thảo, lưu trữ tài liệu có nội dung BMNN trên máy tính hoặc thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông, trừ trường hợp lưu giữ BMNN theo quy định của pháp luật về cơ yếu

- Truyền đưa BMNN trên phương tiện thông tin, viễn thông trái với quy định của pháp luật cơ yếu.

- Chuyển mục đích sử dụng máy tính, thiết bị khác đã dùng để soạn thảo, lưu trữ, trao đổi BMNN khi chưa loại bỏ BMNN

- Sử dụng thiết bị có tính năng thu, phát tín hiệu, ghi âm, ghi hình trong hội nghị, hội thảo, cuộc họp có nội dung BMNN dưới mọi hình thức khi chưa được người có thẩm quyền cho phép

- Đăng tải, tán phát BMNN trên phương tiện thông tin đại chúng, mạng Internet, mạng máy tính và mạng viễn thông".

Chỉ thị số 02/CT-BCA ngày 27/4/2021 của Bộ Công an về tăng cường công tác phòng, chống tấn công mạng và bảo vệ BMNN trên không gian mạng trong Công an nhân dân nêu rõ một số hành vi bị nghiêm cấm trong sử dụng các thiết bị, phương tiện điện tử liên quan đến BMNN:

Nghiêm cấm soạn thảo, lưu trữ văn bản nội bộ, thông tin thuộc BMNN trên máy tính hoặc các thiết bị khác có kết nối mạng Internet.

Nghiêm cấm sử dụng USB, ổ cứng di động và các thiết bị lưu trữ khác có khả năng tự sao chép dữ liệu để chuyển dữ liệu giữa các máy tính nghiệp vụ và giữa máy tính nghiệp cụ với máy tính có kết nối Internet. Trường hợp cần thiết thì phải sử dụng đĩa CD/DVD và phải hủy sau khi sử dụng.

Không sử dụng micro vô tuyến, máy tính, máy tính bảng, điện thoại di động, thiết bị ghi âm, thu phát tín hiệu có khả năng kết nối Internet trong các cuộc họp có nộ dung BMNN. Không đưa vào sử dụng các trang thiết bị kỹ thuật thông tin liên lạc do các tổ chức, cá nhân trong và ngoài nước tài trợ, tăng,… khi chưa được kiểm tra an ninh mạng.

Cán bộ, chiến sĩ không sử dụng các thiết bi có tính năng kết nối Internet quay phim, chụp ảnh, đăng tải hình ảnh cơ quan, đơn vị, địa điểm chứa đựng BMNN lên mạng Internet".

b. Nhóm các văn bản quy định về biện pháp xử lý đối với các hành vi làm lộ BMNN

- Về xử lý hình sự:

Bộ luật Hình sự năm 2015 có 03 điều quy định trực tiếp đối với các hành vi xâm hại BMNN, gồm: Điều 110 (Tội gián điệp), Điều 337 (Tội cố ý làm lộ BMNN; tội chiếm đoạt, mua bán, tiêu hủy tài liệu BMNN); Điều 338 (Tội vô ý làm lộ BMNN; tội làm mất vật, tài liệu BMNN); 06 điều quy định về các hành vi xâm hại đến bí mật công tác, bí mật quân sự, gồm: Điều 361 (Tội cố ý làm lộ bí mật công tác; tội chiếm đoạt, mua bán hoặc tiêu hủy tài liệu bí mật công tác); Điều 362 (Tội vô ý làm lộ bí mật công tác; tội làm mất tài liệu bí mật công tác); Điều 404 (Tội cố ý làm lộ bí mật công tác quân sự); Điều 405 (Tội chiếm đoạt, mua bán hoặc tiêu hủy tài liệu bí mật công tác quân sự); Điều 406 (Tội vô ý làm lộ bí mật công tác quân sự); Điều 407 (Tội làm mất tài liệu bí mật công tác quân sự).

Ngoài ra, còn có 04 điều quy định về các hành vi xâm hại đến mạng máy tính, viễn thông, internet, như: 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 289 (Tội xâm nhập trái phép vào mạng máy tính, mạng viễn thông hoặc phương tiện điện tử của người khác). Đây là môi trường mà lưu lượng thông tin được trao đổi rất lớn, trong đó có cả những thông tin

BMNN bị rò rỉ, bị lấy cắp, chiếm đoạt…

- Về xử lý hành chính: Tại Điều 19, Nghị định 144/2021/NĐ-CP ngày 31/12/2021 của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh, trật tự, an toàn xã hội; phòng, chống tệ nạn xã hội; phòng cháy, chữa cháy; cứu nạn, cứu hộ; phòng, chống bạo lực gia đình đã quy định các mức xử phạt vi phạm hành chính liên quan đến bảo vệ BMNN:

1. Phạt tiền từ 1.000.000 đồng đến 3.000.000 đồng đối với một trong những hành vi sau đây:

a) Không ban hành quy chế, nội quy bảo vệ BMNN trong cơ quan, tổ chức, địa phương theo quy định của pháp luật;

b) Sao, chụp, lưu giữ, vận chuyển, giao, nhận tài liệu, vật chứa BMNN không đúng quy định của pháp luật;

c) Không thu hồi tài liệu, vật chứa BMNN theo quy định của pháp luật;

d) Mang tài liệu, vật chứa BMNN ra khỏi nơi lưu giữ phục vụ công tác mà không được phép của người có thẩm quyền;

đ) Không bàn giao tài liệu, vật chứa BMNN khi thôi việc, chuyển công tác, nghỉ hưu, không được phân công tiếp tục quản lý BMNN;

e) Sử dụng BMNN không đúng mục đích;

g) Xác định BMNN đối với tài liệu không chứa nội dung BMNN, đóng dấu chỉ độ mật lên tài liệu không chứa nội dung BMNN không đúng quy định của pháp luật;

h) Xác định sai độ mật theo quy định của pháp luật;

i) Không xác định, đóng dấu chỉ độ mật BMNN theo quy định của pháp luật.

2. Phạt tiền từ 3.000.000 đồng đến 5.000.000 đồng đối với một trong những hành vi sau đây:

a) Thu thập BMNN không đúng quy định của pháp luật;

b) Không thực hiện biện pháp ngăn chặn, khắc phục hậu quả khi để xảy ra lộ, mất BMNN;

c) Không thông báo với cơ quan, người có thẩm quyền khi xảy ra lộ, mất BMNN;

d) Không loại bỏ BMNN khi chuyển mục đích sử dụng máy tính, thiết bị khác đã dùng để soạn thảo, lưu giữ, trao đổi BMNN;

đ) Tiêu hủy tài liệu, vật chứa BMNN không đúng quy định của pháp luật.

3. Phạt tiền từ 5.000.000 đồng đến 10.000.000 đồng đối với một trong những hành vi sau đây:

a) Soạn thảo, lưu giữ tài liệu có chứa nội dung BMNN trên máy tính hoặc thiết bị khác đã kết nối hoặc đang kết nối với mạng Internet, mạng máy tính, mạng viễn thông không đúng quy định của pháp luật;

b) Sử dụng thiết bị có tính năng thu, phát tín hiệu, ghi âm, ghi hình hoặc hình thức khác trong hội nghị, hội thảo, cuộc họp có nội dung BMNN mà không được phép của người có thẩm quyền;

c) Làm sai lệch, hư hỏng tài liệu, vật chứa BMNN;

d) Cung cấp, chuyển giao BMNN không đúng quy định của pháp luật;

đ) Vào địa điểm lưu giữ, bảo quản BMNN hoặc quay phim, chụp ảnh, vẽ sơ đồ địa điểm lưu giữ, bảo quản BMNN mà không được phép của người có thẩm quyền.

4. Phạt tiền từ 20.000.000 đồng đến 30.000.000 đồng đối với một trong những hành vi sau đây:

a) Làm lộ BMNN; làm mất tài liệu, vật chứa BMNN nhưng chưa đến mức truy cứu trách nhiệm hình sự;

b) Đăng tải, phát tán BMNN trên phương tiện thông tin đại chúng, mạng Internet, mạng máy tính và mạng viễn thông không đúng quy định của pháp luật;

c) Truyền đưa BMNN trên phương tiện thông tin, viễn thông không đúng quy định của pháp luật.

5. Hình thức phạt bổ sung

Tịch thu tang vật, phương tiện vi phạm hành chính đối với hành vi quy định tại điểm b, đ khoản 3 Điều này.

6. Biện pháp khắc phục hậu quả:

a) Buộc nộp lại tài liệu, vật chứa BMNN đối với hành vi quy định tại các điểm b, d, đ và e khoản 1; điểm a khoản 2 và điểm d khoản 3 Điều này;

b) Buộc thu hồi tài liệu, vật chứa BMNN đối với hành vi quy định tại điểm c khoản 1 Điều này;

c) Buộc gỡ bỏ tài liệu BMNN đối với hành vi quy định tại điểm a khoản 3 và các điểm b và c khoản 4 Điều này;

d) Buộc khôi phục lại tình trạng ban đầu đối với hành vi quy định tại điểm c khoản 3 Điều này.

II. KHÔNG GIAN MẠNG VÀ NHỮNG RỦI RO ĐỐI VỚI BÍ MẬT NHÀ NƯỚC

1. Khái niệm

Theo khoản 3 Điều 2 Luật An ninh mạng 2018, không gian mạng là mạng lưới kết nối của cơ sở hạ tầng công nghệ thông tin, bao gồm mạng viễn thông, mạng Internet, mạng máy tính, hệ thống thông tin, hệ thống xử lý và điều khiển thông tin, cơ sở dữ liệu; là nơi con người thực hiện các hành vi xã hội không bị giới hạn bởi không gian và thời gian.

Nói cách khác, không gian mạng là môi trường do công nghệ thông tin tạo ra, trong đó bao gồm các hệ thống mạng, thiết bị kết nối, dữ liệu và các hoạt động trên môi trường số.

2. Đặc điểm của không gian mạng

a. Không gian mạng không có biên giới.

Trên không gian mạng con người tạo ra một "không gian ảo" với các "xa lộ thông tin toàn cầu", hoàn toàn không có biên giới ngăn cách. Chỉ cần sở hữu một thiết bị điện tử có khả năng kết nối internet, người dùng có thể cập nhật thông tin ở bất cứ nơi đâu, bất cứ lúc nào, thậm chí truy cập vào bất kỳ kho tư liệu nào trên thế giới. Trên không gian mạng, chủ đề, lĩnh vực, nội dung nào cũng có thể ngay lập tức được đăng tải và tiếp cận tới hàng tỷ người, khiến những rào cản thông thường như biên giới quốc gia, ngôn ngữ trở nên mỏng manh.

b. Không gian mạng là "sân chơi" thông tin của cả cộng đồng.

Trên không gian mạng, mỗi cá nhân đều có hai vai trò chủ đạo: người cung cấp thông tin và người tiếp cận thông tin. Thông tin trên không gian mạng rất đa chiều, từ nhiều nguồn khác nhau nên đòi hỏi người tiếp nhận thông tin phải thông thái, sáng suốt để chắt lọc thông tin phù hợp và luôn trau dồi bản thân, tự trang bị cho mình những kiến thức, kỹ năng và ý thức trách nhiệm khi tham gia tương tác trên không gian mạng.

c. Không gian mạng có khả năng đa phương tiện, tương tác cao, liên kết và lan tỏa nhanh chóng.

Nhờ cấu trúc, tính năng của các diễn đàn, mạng xã hội, trang chia sẻ,.. Mà người sử dụng có thể tìm kiếm, theo dõi các hoạt động của nhau và tham gia vào các hoạt động khác như đăng bài viết, bình luận, chia sẻ,… một cách thuận lợi, dễ

dàng. Nhờ sự gia tăng liên tục các hoạt động đăng tải, chia sẽ và lưu trữ thông tin của hàng tỷ người trên thế giới với nhiều hình thức văn bản, âm thanh, hình ảnh, video,… đã làm cho thông tin trên không gian mạng trở nên vô cùng phong phú.

d. Không gian mạng không có bộ lọc, trong khi ảnh hưởng, tác động đến cuộc sống xã hội thì ngay lập tức.

Không gian mạng là môi trường sinh hoạt ảo dành cho tất cả mọi người. Do không giới hạn người dùng nên bất kỳ ai cũng có thể tham gia vào môi trường này, không phân biệt tôn giáo, sắc tộc, tuổi tác, giới tính, hay trình độ văn hóa. Từ những thông tin có giá trị đến những thông tin có tính chất suy đồi, vô văn hóa đều xuất hiện trên không gian mạng và dễ truy cập, sử dụng một cách miễn phí. Vì vậy, thông tin trên không gian mạng thật - giả lẫn lộn, thiếu chính xác, khó kiểm chứng, gia tăng nguy cơ lộ lọt bí mật cá nhân, suy giảm quyền lực nhà nước và sức mạnh quốc gia. Thông tin giả trên không gian mạng đang là vấn nạn lớn của nhiều quốc gia, tác động tiêu cực đến cộng đồng, tạo ra những hệ lụy khôn lường, nhất là trong bối cảnh xung đột, khủng bố, dịch bệnh đang diễn ra ngày càng khốc liệt.

3. Những rủi ro tiềm ẩn đối với BMNN trên không gian mạng

Không gian mạng đóng vai trò quan trọng trong việc bảo vệ và đảm bảo an toàn cho hệ thống thông tin, bao gồm các dữ liệu quan trọng của cơ quan nhà nước. Tuy nhiên, sự phát triển của công nghệ cũng mang đến nhiều rủi ro, đặc biệt là nguy cơ tấn công mạng nhằm tiếp cận BMNN, bao gồm:

Tấn công mạng có chủ đích (APT - Advanced Persistent Threats): Đây là hình thức tấn công tinh vi, trong đó kẻ xấu sử dụng các phương thức như lừa đảo, khai thác lỗ hổng bảo mật, hoặc cài đặt mã độc để xâm nhập vào hệ thống của cơ quan nhà nước. Sau khi xâm nhập thành công, chúng có thể ẩn nấp trong thời gian dài, liên tục theo dõi, thu thập thông tin mật hoặc gây rối loạn hệ thống bằng cách phá hủy hoặc chỉnh sửa dữ liệu quan trọng.

Rò rỉ thông tin từ nội bộ: Cán bộ, nhân viên có quyền tiếp cận BMNN có thể vô tình hoặc cố ý để lộ thông tin qua email công việc không được mã hóa, tin nhắn trên các ứng dụng không bảo mật hoặc sao chép dữ liệu vào thiết bị cá nhân như USB, máy tính xách tay không có biện pháp bảo vệ. Các đối tượng gián điệp có thể lợi dụng kỹ thuật tấn công phi kỹ thuật (social engineering), như giả mạo danh tính, tạo email lừa đảo hoặc sử dụng các biện pháp tâm lý để lừa nhân viên tiết lộ thông tin mật.

Phần mềm độc hại và mã độc gián điệp: Các loại virus, mã độc có thể bị cài cắm vào hệ thống thông qua email giả mạo, liên kết độc hại hoặc phần mềm không

rõ nguồn gốc. Một số mã độc có thể âm thầm theo dõi hoạt động của hệ thống, thu thập dữ liệu nhạy cảm và gửi về máy chủ điều khiển từ xa. Ngoài ra, có những mã độc được thiết kế để mã hóa dữ liệu, yêu cầu tiền chuộc (ransomware) hoặc phá hủy hoàn toàn thông tin BMNN, gây hậu quả nghiêm trọng đến an ninh quốc gia..

Thiết bị công nghệ kém bảo mật: Việc sử dụng điện thoại, máy tính cá nhân hoặc thiết bị lưu trữ di động không được kiểm soát có thể tạo ra lỗ hổng bảo mật nghiêm trọng. Những thiết bị này có thể bị nhiễm phần mềm gián điệp, bị tấn công từ xa hoặc vô tình kết nối với mạng không an toàn, tạo điều kiện cho kẻ xấu xâm nhập và đánh cắp BMNN. Ngoài ra, việc sao chép dữ liệu vào USB hoặc ổ cứng di động không được mã hóa cũng có thể dẫn đến mất mát hoặc rò rỉ thông tin quan trọng.

Giả mạo và tấn công lừa đảo (phishing, social engineering): Tội phạm có thể giả mạo email của cơ quan nhà nước, tạo các trang web có giao diện tương tự cổng thông tin chính thống hoặc sử dụng tài khoản mạng xã hội mạo danh lãnh đạo, cán bộ để gửi yêu cầu cung cấp dữ liệu BMNN. Chúng có thể sử dụng các thủ đoạn như gửi email chứa liên kết độc hại, yêu cầu đăng nhập vào hệ thống giả mạo hoặc dụ dỗ nhân viên cung cấp thông tin mật qua các cuộc trò chuyện trực tuyến.

CHƯƠNG 2. NHỮNG NGUY CƠ VÀ THÁCH THỨC TRONG BẢO VỆ BÍ MẬT NHÀ NƯỚC TRÊN KHÔNG GIAN MẠNG

I. NHỮNG PHƯƠNG THỨC, THỦ ĐOẠN CỦA TỘI PHẠM TẤN CÔNG MẠNG GÂY LỘ, LỌT, MẤT BÍ MẬT NHÀ NƯỚC

1. Tình hình an ninh mạng trên thế giới

Tình hình an ninh mạng trên thế giới diễn biến rất phức tạp, nhất là các hoạt động mua bán, trao đổi dữ liệu trên không gian mạng.

Các nhóm gián điệp mạng với sự hậu thuẫn của chính phủ các nước gia tăng hoạt động, thực hiện các chiến dịch tấn công mạng nhằm vào hạ tầng thông tin trọng yếu để đánh cắp thông tin, tài liệu. Hệ thống mạng của Bộ Ngoại giao Canada, Tổng cục tình báo (DIGIMIN) của Peru, Quốc hội Slovakia và Ba Lan, Bộ Quốc phòng Australia, Đại học Công nghiệp Tây Bắc của Trung Quốc, Hệ thống Internet tại Triều Tiên, Mạng viễn thông Vodafone của Bồ Đào Nha… bị các nhóm gián điệp mạng xâm nhập, kiểm soát. Các nhóm tin tặc có sự hậu thuẫn của chính phủ các nước, như: Trung Quốc (Hafnium APT, Mustang Panda, Cicada, Winti, APT 10, DEV-040), Nga (APT28, Conti, RedBanditsRU, UNC1151, Gamaredon, Sandworm), Triều Tiên (APT37), Palestine (APT-C-23)… thực hiện hoạt động tấn công mạng nhằm vào hệ thống mạng, cơ quan chính phủ, tổ chức, cá nhân ở các nước có xung đột về chính trị, quân sự, lợi ích quốc gia.

Các quốc gia, tổ chức quốc tế ban hành các chính sách quản lý tăng cường bảo đảm an ninh mạng. Nga thành lập Ủy ban liên Bộ đảm bảo chủ quyền công nghệ trong lĩnh vực phát triển cơ sở hạ tầng thông tin trọng yếu quốc gia; Trung Quốc tăng cường giám sát hoạt động của các Công ty công nghệ trong nước và nước ngoài, kiểm soát nội dung phát trực tiếp (livestream) trên các nền tảng mạng xã hội; Mỹ thông qua 03 Đạo luật về cơ chế chia sẻ công cụ và giao thức bảo mật, tăng cường bảo đảm an ninh mạng cho các hệ thống điều khiển công nghiệp và kiểm soát nội dung vi phạm pháp luật trên Internet; Nhật Bản yêu cầu các doanh nghiệp có hạ tầng thông tin trọng yếu tăng cường các biện pháp bảo vệ an ninh mạng; Úc ban hành Dự luật Bảo vệ quyền riêng tư sửa đổi, gia tăng hình phạt cho hành vi vi phạm gây rò rỉ thông tin; Singapore thành lập lực lượng đặc nhiệm liên ngành để đối phó với tội phạm mạng.

Các nhóm tin tặc xâm nhập, đánh cắp thông tin của các tổ chức nhà nước, tập đoàn kinh tế và rao bán trên quy mô lớn. 23 TB dữ liệu chứa thông tin của 01 tỷ công dân Trung Quốc; 800 triệu bản ghi thông tin nhận dạng khuôn mặt và biển số phương tiện giao thông của công dân Trung Quốc; 34 GB dữ liệu

của 1,37 tỷ tài khoản người dùng TikTok, WeChat trên thế giới bị tin tặc đánh cắp, rao bán. Ngoài ra, các cơ quan, tổ chức hoạt động trong lĩnh vực năng lượng, viễn thông quan trọng của các nước cũng bị tấn công mạng, đánh cắp thông tin, mã hóa dữ liệu tống tiền. Cơ quan quản lý hệ thống điện của Ý bị đánh cắp hơn 700 GB dữ liệu; Công ty điều hành đường ống dẫn khí đốt tự nhiên quốc gia Hy Lạp DESFA bị đánh cắp 361 GB dữ liệu… Nền tảng truyền thông trực tuyến "START" của Nga bị đánh cắp cơ sở dữ liệu của 7,5 triệu người dùng; Công ty viễn thông Optus lớn nhất của Úc đã bị đánh cắp thông tin cá nhân của hơn 10 triệu khách hàng.

Xu hướng tấn công mạng qua chuỗi cung ứng ngày càng gia tăng, các ứng dụng phổ biến tồn tại các lỗ hổng bảo mật nghiêm trọng, nguy cơ ảnh hưởng tới hàng triệu người dùng trên thế giới. Ứng dụng TikTok trên hệ điều hành Android với hơn 1,5 tỷ lượt tải xuống tồn tại lỗ hổng bảo mật cho phép tin tặc chiếm đoạt tài khoản người dùng; Microsoft xác nhận 02 lỗ hổng bảo mật nghiêm trọng tồn tại trên máy chủ thư điện tử Microsoft Exchange bị tin tặc khai thác trong các chiến dịch tấn công mạng có chủ đích; lỗ hổng bảo mật nghiêm trọng tồn tại trên phần sụn (firmware) của các thiết bị tường lửa thuộc hãng Sophos, Juniper và hàng triệu thiết bị của hãng HP, Dell, Intel, Microsoft, Fujitsu, Framework, Siemens nguy cơ bị tin tặc khai thác, tấn công, xâm nhập hệ thống mạng các tổ chức, doanh nghiệp trên toàn thế giới.

2. Tình hình sử dụng không gian số ở Việt Nam

Là một trong các quốc gia có tốc độ phát triển Internet nhanh nhất thế giới, Việt Nam có nhiều tiềm năng, điều kiện thuận lợi thực hiện công cuộc chuyển đổi số quốc gia.

Theo We Are Social thống kê, thông tin chi tiết người dân Việt Nam sử dụng các thiết bị và dịch vụ kỹ thuật số để kết nối với nhau trong những năm qua, có thể thấy số lượng người dùng Internet lẫn tỷ lệ người dùng so với tổng dân số đều có sự tăng trưởng, là bằng chứng rõ rệt cho thấy thị trường Internet tại Việt Nam đầu năm 2025 đã có sự phát triển hơn so với năm trước.

Mặt khác, người dân tại Việt Nam có xu hướng ngày càng sở hữu nhiều thiết bị di động hơn, khi số lượng thiết bị mà mỗi người dân đang sở hữu vào năm 2025 vẫn tăng cao hơn so với năm trước.

Theo We Are Social, tổng dân số Việt Nam tính đến tháng 4/2024 là hơn 101 triệu người, trong đó, 50.2% dân số là nữ giới, đồng thời, 39.1% dân số tập trung ở vùng thành thị. Tính đến đầu năm 2025, Việt Nam có 80 triệu người sử

dụng Internet, tương đương 80% so với tổng dân số, dự báo đến năm 2029 số lượng người dùng internet sẽ tăng vượt mốc 100 triệu người .

Về thời gian sử dụng Internet mỗi ngày, báo cáo của We Are Social cho thấy, trong mỗi ngày trung bình người dùng tại Việt Nam dành khoảng 6 giờ 23 phút để lướt Internet, trong đó 55.4% thời gian sử dụng Internet thông qua các thiết bị di động. Trong đó, thời gian trung bình dành cho mạng xã hội và các ứng dụng nhắn tin là khoảng 2 giờ 32 phút mỗi ngày.

Sau gần 30 năm kết nối với mạng Internet toàn cầu, Việt Nam đã chứng kiến những bước phát triển ngoạn mục, chưa từng có nhờ những quyết sách, định hướng đúng đắn của Đảng, Nhà nước về phát triển công nghệ thông tin (CNTT), viễn thông, Internet; đồng thời, đứng trước những thời cơ, vận hội mới để đi tắt đón đầu, tranh thủ những thành tựu khoa học và công nghệ tiên tiến nhằm đẩy nhanh hơn tiến trình công nghiệp hóa, hiện đại hóa đất nước, hội nhập sâu rộng, hiệu quả hơn vào nền kinh tế thế giới, không ngừng nâng cao tiềm lực về quốc phòng, an ninh.

Không thể phủ nhận Chuyển đổi số mang lại lợi ích to lớn cho quốc gia, dân tộc, tuy nhiên, với tiềm lực quốc gia về an ninh mạng chưa đủ mạnh, hạ tầng công nghệ còn hạn chế, phụ thuộc rất lớn vào công nghệ nước ngoài, nước ta đang đối mặt với nhiều thách thức trong bảo đảm an ninh mạng và phòng, chống tội phạm sử dụng công nghệ cao. Điển hình là:

- Nguy cơ mất tự chủ, bị lệ thuộc vào công nghệ nước ngoài, tụt hậu;

- Thách thức từ các cuộc tấn công mạng nhằm vào cơ sở hạ tầng thông tin trọng yếu quốc gia; cũng như công tác bảo đảm an ninh hệ thống mạng thông tin trọng yếu tại các cơ quan, bộ, ngành chưa được quan tâm đúng mức: Công tác phòng ngừa, đảm bảo an ninh hệ thống mạng tại một số cơ quan, đơn vị chủ quản chưa được quan tâm triển khai đúng mức, công tác kiểm tra, đánh giá an ninh hệ thống mạng chưa được chú trọng; việc đầu tư hệ thống kỹ thuật, giải pháp bảo đảm an ninh, an toàn chưa đồng bộ, chưa đáp ứng yêu cầu đặt ra.

- Nguy cơ Mạng xã hội xuyên biên giới tác động tiêu cực đến vai trò của cơ quan truyền thông chính thống trong nước: Phát hiện gần 5.000 mục tiêu trọng điểm đăng tải hơn 116.200 tin, bài viết gốc chống phá, thu hút hơn 364 triệu người xem, bình luận, chia sẻ; Hoạt động báo chí và các phương tiện truyền thông chậm đổi mới về hình thức truyền thông

- Tội phạm mạng, tội phạm sử dụng công nghệ cao có xu hướng gia tăng

Trong năm 2022, bằng các biện pháp nghiệp vụ, cục An ninh mạng A05 đã phát hiện **3,09 triệu** thư điện tử lừa đảo đính kèm đường dẫn, tệp tin mã độc được phát tán trên mạng tại Việt Nam, nhiều nhất trong các nước khu vực châu Á - Thái Bình Dương; hơn 7.394 thiết bị camera Hikvision tại Việt Nam tồn tại lỗ hổng bảo mật cho phép tin tặc truy cập trái phép camera của người dùng cá nhân, tổ chức; 261 máy chủ phần mềm quản lý dữ liệu kế toán của các cơ quan, doanh nghiệp tại Việt Nam bị lây nhiễm các biến thể mã độc tống tiền, được phát tán từ 6.000 địa chỉ IP của tin tặc. Đáng chú ý, qua công tác bảo đảm an ninh hệ thống mạng thông tin quốc gia, phát hiện lỗ hổng bảo mật nghiêm trọng trên Cổng dịch vụ công trực tuyến của Bộ Công an, Bộ Thông tin và Truyền thông, và 32 UBND tỉnh/thành phố do Tập đoàn Bưu chính Viễn thông Việt Nam (VNPT) phát triển cho phép tin tặc khai thác, đánh cắp thông tin, dữ liệu của người dân đăng ký hồ sơ dịch vụ công.

Tại các diễn đàn trên không gian mạng, thông tin, dữ liệu của các cơ quan, tổ chức, cá nhân bị rao bán công khai: 3,9 triệu bản ghi dữ liệu của giáo viên, sinh viên, học sinh Việt Nam; 6,2 triệu bản ghi dữ liệu liên quan việc đặt vé máy bay của các khách hàng Hãng hàng không Vietjet Air; 1,2 triệu thông tin khách hàng của Công ty Cổ phần chứng khoán VNDirect; 600 nghìn bản ghi dữ liệu của một Công ty thời trang tại Việt Nam; cơ sở dữ liệu cá nhân của 50 nghìn cư dân khu đô thị Ecopark; dữ liệu của Học viện Cảnh sát nhân dân.

Các chuyên gia cho biết, tính đến tháng 6/2023, Việt Nam xếp thứ 12 trên thế giới về tỷ lệ người dùng Internet; số lượng thuê bao di động được đăng ký lên đến hơn 156 triệu thuê bao; xếp hạng thứ 25 về chỉ số an toàn, an ninh mạng toàn cầu (do Liên minh Viễn thông quốc tế ITU công bố). Tuy nhiên, theo thống kê của các hãng bảo mật quốc tế, Việt Nam nằm trong nhóm 3 quốc gia bị tấn công mạng nhiều nhất tại khu vực châu Á - Thái Bình Dương; chỉ riêng 6 tháng đầu năm 2023, các cơ quan chức năng đã phát hiện gần 17 triệu cảnh báo dấu hiệu hoạt động tấn công mạng (tăng 240% so với cùng kỳ năm 2022), trong đó có 208 hệ thống thông tin của cơ quan Nhà nước, các bộ, ban, ngành bị tin tặc tấn công nhằm mục đích đánh cắp thông tin, dữ liệu, tài liệu BMNN thuộc nhiều lĩnh vực. Nổi lên là các chiến dịch tấn công mạng nguy hiểm của các tin tặc có nguồn gốc từ nước ngoài, sử dụng 15 biến thể mã độc nguy hiểm, trong đó có các loại mã độc hiện đại, có khả năng vô hiệu hóa các phần mềm bảo vệ để "nằm vùng" lâu dài, thâm nhập sâu vào các hệ thống, đáng chú ý có sự câu kết, móc nối giữa tin tặc trong và ngoài nước.

Cơ quan chức năng cũng phát hiện hơn 4.000 nguồn khởi phát thông tin

xấu độc, thu hút hơn 82 triệu lượt tiếp cận, tương tác thông tin, chủ yếu trên các nền tảng mạng xã hội, với hàng nghìn tài khoản, "hội nhóm" có hàng triệu lượt người theo dõi. Tình trạng lộ, mất tài liệu BMNN trên không gian mạng tiếp tục được phát hiện, trong 3 năm qua, cơ quan chức năng đã phát hiện, xử lý hơn 150 vụ việc với 710 đầu tài liệu bị lộ, trong đó có nhiều tài liệu thuộc danh mục tài liệu mật, tối mật, tuyệt mật. Trong 6 tháng đầu năm 2023, đã phát hiện 25 vụ đăng tải, truyền đưa thông tin, tài liệu BMNN trên không gian mạng với 58 đầu tài liệu mật; hơn 200 GB dữ liệu nội bộ, tài liệu nhạy cảm của các cơ quan, đơn vị thuộc các bộ, ngành, địa phương bị lộ lọt, rao bán trên các diễn đàn, hội nhóm.

Trong thời gian qua, Bộ Công an phát hiện hàng trăm cá nhân, tổ chức liên quan bán dữ liệu cá nhân. Một số đường dây chiếm đoạt, mua bán dữ liệu quy mô lớn tại Việt Nam đã bị phát hiện, đấu tranh, xử lý. Số lượng dữ liệu cá nhân bị thu thập, mua bán trái phép phát hiện được lên tới gần 1.300 GB, trong đó có nhiều dữ liệu cá nhân nội bộ, nhạy cảm.

3. Một số phương thức, thủ đoạn của tội phạm tấn công mạng gây lộ, lọt, mất bí mật nhà nước

Thời gian qua, tình hình an ninh mạng trên thế giới và trong nước tiếp tục diễn biến phức tạp. Xuất hiện ngày càng nhiều các vụ tấn công mạng khai thác lỗ hổng bảo mật các ứng dụng nhằm xâm nhập hệ thống máy tính của các cơ quan và cá nhân; phát tán mã độc quy mô toàn cầu với mục tiêu tấn công đa dạng, không tập trung. Các nhóm tin tặc lợi dụng tình hình phức tạp của dịch bệnh hậu Covid-19, xung đột Nga-Ukraine, Israel-Palestins, công cuộc cải cách bộ máy hành chính của Nhà nước ta để tấn công mạng bằng cách tạo ra các ứng dụng truy vết, gửi thông tin, tài liệu giả mạo để phát tán mã độc. Nhiều vụ lộ, rò rỉ thông tin, dữ liệu nhạy cảm tiếp tục được công bố hoặc rao bán công khai trên các diễn đàn. Một số vụ việc nổi bật như:

Khai thác lỗ hổng bảo mật (Zero-day) một số dịch vụ, ứng dụng phổ biến; thiết bị định tuyến tồn tại lỗ hổng bảo mật;

Giả mạo thông tin về dịch bệnh COVID-19, xung đột Nga-Ukraine, Israel-Palestins đính kèm mã độc phát tán tới các cơ quan, tổ chức;

Rao bán dữ liệu của 1 tỷ công dân Trung Quốc hay dữ liệu cá nhân của 30 triệu sinh viên, học sinh Việt Nam…

Với tốc độ phát triển và ứng dụng công nghệ thông tin nhanh chóng như hiện nay, tình hình an ninh mạng của Việt Nam sẽ tiếp tục có nhiều diễn biến phức tạp, tội phạm mạng tiếp tục gia tăng, hoạt động rộng khắp trên mọi lĩnh vực,

trong đó có nhiều vụ làm lộ, lọt và mất BMNN.

Qua đó, phát hiện các nhóm gián điệp mạng *sử dụng nhiều phương thức tấn công, xâm nhập tinh vi đa dạng, cá nhân hóa theo đối tượng*, như:

Gửi thư điện tử giả mạo, nhắn tin lừa đảo thông qua mạng xã hội (Facebook), SMS; dẫn dụ kích hoạt mã độc trên các thiết bị điện tử;

Khai thác lỗ hổng bảo mật của các ứng dụng văn phòng để cài cắm mã độc vào các tệp tin văn bản và các phần mềm ứng dụng phổ biến;

Tấn công chiếm quyền điều khiển thiết bị định tuyến, chuyển hướng truy cập mạng đến máy chủ chứa mã độc;

Khai thác các lỗ hổng bảo mật trên trang, cổng thông tin điện tử công khai trên mạng Internet; leo thang đặc quyền, xâm nhập vào hệ thống mạng nội bộ, chiếm đoạt thông tin, tài liệu;

Tấn công thiết bị điện tử của quản trị mạng, từ đó kiểm soát máy chủ quản trị miền (Domain Controller), lựa chọn mục tiêu máy trạm để lây nhiễm mã độc;

Tấn công kiểm soát hệ thống quản lý mã độc tập trung, lợi dụng chính hệ thống này vào hoạt động phát tán mã độc, kiểm soát các máy trạm trong toàn bộ hệ thống mạng;

Lây nhiễm mã độc vào các thiết bị ngoại vi (USB, Camera, điện thoại thông minh) để thu thập thông tin, tài liệu trong mạng đóng (không kết nối với Internet).

Bên cạnh đó, các nhóm tin tặc, gián điệp mạng nước ngoài cũng thường xuyên ***nghiên cứu ứng dụng kỹ thuật mới vào phát triển các dòng mã độc chuyên biệt*:**

Kích hoạt mã độc bằng các tệp tin "sạch" có chữ ký số hợp lệ; tải và thực thi tiến trình mã độc trên bộ nhớ tạm, không lưu mã độc trên ổ cứng;

Tối ưu và đơn giản hóa mã độc (không thường trú trên máy tính, điện thoại nạn nhân mà chỉ nằm vùng ở một số vị trí nhất định, sử dụng các đoạn mã không độc hại như lệnh tìm kiếm, sao chép, nén tệp tin để qua mặt tường lửa, phần mềm bảo mật);

Mã độc sử dụng trí tuệ nhân tạo (AI) tự động lây nhiễm và hoạt động mà không cần kết nối máy chủ điều khiển trong các mạng nội bộ; tìm kiếm các kết nối đồng thời cả hệ thống mạng nội bộ và mạng Internet để chuyển dữ liệu ra ngoài Internet.

Sau khi xâm nhập, chiếm quyền điều khiển thành công thiết bị điện tử, ***các***

dòng mã độc đều có tính năng thực hiện thủ đoạn gián điệp mạng: tìm kiếm, đánh cắp thông tin, tài liệu; chiếm đoạt tài khoản mạng xã hội (tài khoản/mật khẩu); giám sát quá trình sử dụng thiết bị (kích hoạt micro, camera để chụp màn hình, quay video, ghi âm môi trường xung quanh, xác định vị trí). Đối với các máy tính trong mạng nội bộ, không kết nối Internet, gián điệp mạng sử dụng mã độc nhúng trí tuệ nhân tạo tự động thu thập thông tin về hệ thống mạng, lây nhiễm sang các máy tính trong mạng; thu thập thông tin, tài liệu, lựa chọn mục tiêu làm điểm trung chuyển, lưu vào thư mục ẩn trong thiết bị lưu trữ ngoài (USB, camera, điện thoại thông minh), đợi đến khi khi các thiết bị này kết nối máy tính Internet, dữ liệu sẽ chuyển về máy chủ ở nước ngoài.

II. TÌNH HÌNH LỘ BMNN TRÊN KHÔNG GIAN MẠNG Ở VIỆT NAM THỜI GIAN QUA

1. Lộ BMNN qua đăng tải công khai thông tin, tài liệu BMNN trên các website, cổng thông tin, trang tin điện tử

Trong những năm gần đây, tình hình lộ BMNN qua đăng tải công khai thông tin, tài liệu BMNN trên các website, công thông tin, trang tin điện tử có chiều hướng gia tăng. Theo thống kê của Bộ Công an, trong giai đoạn 2016-2024, có hơn 1000 vụ lộ BMNN, trong đó có nhiều vụ xảy ra do đăng tải công khai thông tin, tài liệu BMNN trên các website, cổng thông tin, trang tin điện tử.

Đây là dạng lộ BMNN trên không gian mạng xảy ra phổ biến nhất thời gian qua. Chỉ tính riêng năm 2022, lực lượng chức năng đã phát hiện 58 vụ lộ BMNN trên trang thông tin điện tử, cổng thông tin điện tử của các cơ quan ban ngành trên tổng số 86 vụ lộ BMNN trên mạng Internet (chiếm 57,57%). Trong đó, tập trung chủ yếu ở các cơ quan, đơn vị cấp cơ sở (cấp huyện chiếm chiếm 37%, cấp tỉnh chiếm 58%, cấp Trung ương chiếm 5%. Năm 2023, Cục A05 đã phát hiện 33 vụ đăng tải, truyền đưa tài liệu BMNN (*tăng 22% so với năm 2022)*, với 65 đầu tài liệu (17 Tối mật, 38 Mật, 10 tài liệu nội bộ) trên các trang, cổng TTĐT của một số cơ quan, đơn vị.

Về nội dung BMNN bị lộ: Qua nghiên cứu các vụ lộ BMNN theo dạng này cho thấy, BMNN lộ theo dạng này chủ yếu các thông tin thuộc mức độ mật và tối mật phản ánh về chủ trương, chính sách của Đảng, Nhà nước như năm 2016, trang thông tin điện tử Ủy ban nhân dân huyện Triệu Phong, Quảng trị đăng tải các văn bản của Ủy ban nhân dân huyện chỉ đạo về báo cáo tình hình thực hiện Nghị quyết Hội nghị lần thứ 4 Ban Chấp hành Trung ương Đảng khóa X về Chiến lược biển Việt Nam đến năm 2020, văn bản số 19/BTNMT-TCBHĐVN ngày

25/02/2016 của Bộ Tài nguyên và Môi trường tỉnh Quảng Trị (tài liệu Mật); thông tin phản ánh về phương án, kế hoạch, kết quả công tác đảm bảo an ninh, quốc phòng trên các địa bàn. Ví dụ như trang thông tin điện tử Bảo hiểm xã hội tỉnh Bình Thuận đã đăng tải Kế hoạch số 394/KH-BCH ngày 6/4/2014 của Ban Chỉ huy Quân sự thành phố Phan Thiết về việc "Tổ chức lực lượng sẵn sàng chiến đấu bảo vệ cao điểm II năm 2015" hay cổng thông tin điện tử thành phố Lào Cai đã đăng tải Kế hoạch số 54/KH-UBND ngày 20/02/2017 về diễn tập chiến đấu phòng thủ xã Đồng Tuyển năm 2017.

Các BMNN bị lộ theo dạng này chủ yếu là các văn bản có chứa nội dung BMNN được đăng tải nguyên văn dưới dạng file (.doc) (chủ yếu là các bản dự thảo của văn bản), file PDF hoặc file dạng ảnh (.jpg, jpeg) đăng tải trên các cổng thông tin, trang tin điện tử của các cơ quan, đơn vị, thường không đóng dấu xác định độ mật trên văn bản.

Có nhiều nguyên nhân dẫn đến tình trạng này, trong đó nguyên nhân chủ quan là do ý thức trách nhiệm của một bộ phận cán bộ, công chức, viên chức trong thực hiện công tác bảo vệ BMNN còn chưa cao. Một số cán bộ, công chức, viên chức chưa nắm vững các quy định của pháp luật về bảo vệ BMNN, chưa có ý thức bảo vệ thông tin, tài liệu BMNN, thậm chí còn chủ quan, lơ là, mất cảnh giác trong việc quản lý, sử dụng thông tin, tài liệu BMNN. Ngoài ra, cấp ủy, thủ trưởng các cơ quan, đơn vị trên chưa quan tâm đúng mức đến công tác bảo vệ BMNN, chưa tổ chức quán triệt nghiêm túc các quy định của pháp luật về bảo vệ BMNN. Cá biệt, có những đồng chí lãnh đạo trực tiếp thẩm duyệt nội dung đăng tải trên các cổng thông tin, trang tin điện tử cũng không nắm rõ quy định của pháp luật về bảo vệ BMNN, phê duyệt cho phép đăng tải các bài viết có chứa nội dung thuộc phạm vi BMNN lên Internet.

Nguyên nhân khách quan là do sự phát triển mạnh mẽ của công nghệ thông tin và truyền thông, đặc biệt là mạng internet. Việc đăng tải thông tin, tài liệu trên mạng internet rất dễ dàng và nhanh chóng, chỉ cần một chiếc điện thoại thông minh là có thể ghi âm, ghi hình, chụp ảnh thông tin, tài liệu BMNN.

Các vụ lộ BMNN qua đăng tải công khai thông tin, tài liệu BMNN trên các website, công thông tin, trang tin điện tử đã gây ra nhiều hậu quả nghiêm trọng, ảnh hưởng đến an ninh quốc gia, trật tự an toàn xã hội, gây thiệt hại về kinh tế, uy tín của cơ quan, tổ chức, cá nhân.

Ví dụ:

- Vụ việc một cán bộ thuộc Bộ Quốc phòng đăng tải thông tin, tài liệu

BMNN trên trang cá nhân Facebook năm 2017. Trong vụ việc này, cán bộ đã đăng tải một số thông tin, tài liệu BMNN về hoạt động của lực lượng vũ trang lên trang cá nhân của mình.

2. Lộ BMNN qua sử dụng dịch vụ thư điện tử gửi, nhận tài liệu BMNN

Thời gian qua, lực lượng chức năng đã phát hiện nhiều vụ lộ BMNN thông qua việc sử dụng dịch vụ thư điện tử gửi, nhận tài liệu BMNN.

Về nội dung BMNN bị lộ chủ yếu là các phương án, kế hoạch, báo cáo kết quả hoạt động của một cơ quan, tổ chức, một ngành, một lĩnh vực thuộc phạm vi BMNN. Trong đó, các tài liệu BMNN thường được gửi bằng file word (.doc), file pdf thông qua các địa chỉ mail của một số nhà cung cấp dịch vụ phổ biến ở Việt Nam như Gmail hoặc Yahoo Mail. Ví dụ, như năm 2017, có cá nhân đã sử dụng địa chỉ mail lmpettuan@gmail.com gửi qua hộp thư công vụ của lãnh đạo các đơn vị, địa phương trong huyện Hàm Thuận, tỉnh Bình Thuận công văn số 663/UBND-NC ngày 24/3/2017 của UBND huyện Hàm Thuận về việc ngăn chặn hoạt động tà đạo Pháp Luân Đại Pháp (tài liệu Mật). Hay như năm 2008, Tỉnh ủy Đăk Nông gửi tài liệu "Phân tích một số thủ đoạn kích động, chia rẽ dân tộc của các thế lực thù địch trên địa bàn tỉnh Đăk Nông" qua mail đến hộp thư bachtt26@vnn.vn. Sau đó tài liệu này được gửi đến 18 doanh nghiệp và cá nhân ở nhiều tỉnh, thành trong nước.

Về hình thức tồn tại của BMNN bị lộ qua gửi, nhận thư điện tử chủ yếu là các bản dự thảo, chưa được xác định độ mật. Tuy nhiên, căn cứ vào danh mục BMNN đã ban hành, có thể xác định độ mật cho các tài liệu này bao gồm cả 03 mức độ là Tuyệt mật, Tối mật và Mật.

Nguyên nhân chủ yếu dẫn đến tình trạng lộ BMNN qua sử dụng dịch vụ thư điện tử là do các cá nhân người dùng không tuân thủ quy định của pháp luật về bảo vệ BMNN trong gửi, nhận tài liệu. Theo quy định: "Nội dung BMNN nếu truyền đưa bằng phương tiện viễn thông và máy tính thì phải được mã hoá theo quy định của pháp luật về cơ yếu". Tuy nhiên, khi gửi các tài liệu BMNN qua dịch vụ thư điện tử, người dùng lại không thực hiện thao tác mã hóa theo đúng quy định của pháp luật về cơ yếu dẫn đến để lộ BMNN.

3. Lộ BMNN qua các trang mạng xã hội

Từ năm 2015 đến nay, lực lượng an ninh mạng đã phát hiện và xử lý nhiều vụ lộ BMNN qua các trang mạng xã hội, trong đó có đa phần là các vụ lộ BMNN qua trang mạng xã hội Facebook, Zalo, Telegram... Kết quả nghiên cứu các vụ lộ BMNN qua mạng xã hội cho thấy:

Về các tài khoản mạng xã hội facebook đăng tải nội dung BMNN bao gồm tài khoản của cá nhân và trang fanpage. Về fanpage, chủ yếu là các trang của các tổ chức khủng bố, tổ chức phản động như tài khoản facebook "Việt Tân" của tổ chức khủng bố Việt Tân, tài khoản facebook "Con đường Việt Nam" của tổ chức phản động "Con đường Việt Nam"; "Nhật ký yêu nước", "Lều của đầy tớ"…

Về tài khoản cá nhân đăng tải các nội dung BMNN chủ yếu là của một số đối tượng chống đối, có quan điểm trái chiều với Đảng, Nhà nước như tài khoản facebook "Chinh minh" của đối tượng phản động Phạm Văn Trội, tài khoản facebook "Dạ Thảo" của đối tượng Nguyễn Thị Dạ Thảo, (đối tượng có mối quan hệ mật thiết với Nguyễn Văn Lý, thành viên tổ chức phản động "Hội anh em dân chủ")… Các chủ tài khoản mạng xã hội trên đăng tải nội dung thuộc phạm vi BMNN lên các trang mạng xã hội đều nhằm mục đích tuyên truyền, phá hoại chủ trương, chính sách của Đảng, Nhà nước phục vụ âm mưu, ý đồ chống đối của chúng. Điển hình như, tháng 7/2017, tài khoản facebook "Việt Tân" của tổ chức khủng bố Việt Tân đã đăng tải bài viết "Toàn phụ nữ, trẻ con, người già, nếu sai luật thì bắt bỏ tù, sao lại có hành động bỉ ổi như vậy?"; đồng thời trích dẫn đường link có ảnh chụp Kế hoạch số 06/KH-UBND ngày 08/9/2016 của Ủy ban nhân dân huyện Quỳ Hợp, tỉnh Nghệ An về phòng ngừa, đấu tranh, ngăn chặn hoạt động Pháp Luân Công trái phép trên địa bàn huyện Quỳ Hợp (tài liệu thuộc độ Mật); hay facebook "Dạ Thảo" của đối tượng Nguyễn Thị Dạ Thảo đã đăng tải công văn số 812/CAT-PA81, ngày 27/2/2017 của Công an tỉnh Thừa Thiên Huế đề nghị giám đốc các Ngân hàng chỉ đạo rà soát, theo dõi hoạt động chuyển, nhận tiền của 10 cá nhân có tên trong danh sách kèm theo liên quan đến hoạt động các đối tượng phạm tội trên địa bàn, trong đó có đối tượng Dạ Thảo (Công văn thuộc độ Tuyệt mật).

Ngoài các dạng tài khoản mạng xã hội ở trên, cũng có một số cá nhân chưa nhận thức được đầy đủ về công tác bảo vệ BMNN, không biết nội dung thông tin mình thu được là BMNN đã vô ý đăng tải lên trên các trang mạng xã hội như trường hợp bà Nguyễn Thi Thu Hiền đã sử dụng điện thoại di động quay trụ sở Công an phường Hợp Giang, thành phố Cao Bằng, tỉnh Cao Bằng rồi đăng tải trên tài khoản facebook cá nhân "Triệu Hoàng Kỳ" (Trụ sở Công an phường Hợp Giang, thành phố Cao Bằng được xác định là khu vực cấm).

Vào ngày 7 tháng 7 năm 2023, khoảng 8 giờ sáng, trên mạng xã hội đã xuất hiện hình ảnh chụp đề thi môn Ngữ văn của kỳ thi tốt nghiệp Trung học Phổ thông năm 2023. Trước tình hình này, Bộ Giáo dục và Đào tạo đã khẩn trương chỉ đạo các đơn vị liên quan xác minh, làm rõ. Qua xác minh, Bộ Giáo

dục và Đào tạo xác định, đề thi môn Ngữ văn bị lộ do một cán bộ coi thi tại điểm thi Trường Trung học phổ thông Chuyên Hoàng Văn Thụ, tỉnh Cao Bằng đã chụp ảnh đề thi và gửi cho một người khác.

4. Một số cá nhân, tổ chức lập website mua, bán, trao đổi tài liệu BMNN và lộ BMNN trên các trang báo điện tử

Tính đến cuối năm 2023, lực lượng an ninh mạng đã phát hiện nhiều website do các cá nhân, tổ chức lập ra để mua bán, trao đổi tài liệu thuộc phạm vi BMNN như các website *http://nonghoc.com; http://123doc.org; http://luanan.nlv.gov.vn; http://thuvienphapluat.vn; http://thukyluat.vn* …

BMNN được các website trên đăng tải công khai mua bán, trao đổi chủ yếu là các tài liệu BMNN trên lĩnh vực quốc phòng, an ninh (luận văn, luận án, đề tài nghiên cứu khoa học…). Điển hình như tài khoản có tên "Nguyễn Hạ Vũ" đăng rao bán tài liệu nghiệp vụ tình báo "Tìm hiểu các khía cạnh tâm lý về động cơ cộng tác của lực lượng bí mật với cơ quan tình báo, ý nghĩa của việc nghiên cứu vấn đề với công tác xây dựng, tuyển chọn và lãnh đạo sử dụng lực lượng bí mật của cơ quan tình báo" trên website http://123doc.org. Các nội dung BMNN được đăng tải công khai theo dạng này còn là các văn bản thuộc phạm vi BMNN khác như websitehttp://thuvienphapluat.vn; http://thukyluat.vn đăng tải công khai tài liệu Thông tư số 01/2011/ANTT-BCA ngày 18/01/2011 của Bộ Công an về hoạt động vũ trang canh gác bảo vệ mục tiêu của lực lượng Cảnh sát bảo vệ (tài liệu Mật).

Ngoài ra, cơ quan chức năng của Bộ Công an cũng phát hiện nhiều vụ lộ BMNN qua báo điện tử,

Điển hình như ngày 16/4/2017, lực lượng An ninh phát hiện trên trang www.http://phapluatplus.vn đăng tải bài viết "Công an Cà Mau rút kinh nghiệm sâu sắc vụ công dân bị cấm xuất cảnh" của phóng viên Ngọc Long kèm theo là bản ảnh Công văn số 56/A62.C3-P6 ngày 12/4/2017 của A62; trường hợp Báo điện tử Người đưa tin, Hội Luật gia Việt Nam đăng tải bài viết "xâm hại tình dục trẻ em Thiếu tướng H.S.T lên tiếng" sử dụng hình ảnh đồng chí H.S.T và trên bàn làm việc có bản tin BP3 của ngành (tài liệu Tuyệt mật) hay trường hợp Báo điện tử Vietnamnet đăng tải bài viết "Nhập siêu Trung Quốc tăng 160 lần:15 năm bó tay?" có nhiều nội dung trùng khớp với bản dự thảo báo cáo "Tình hình quan hệ thương mại Việt Nam - Trung Quốc và vấn đề nhập siêu và giải pháp kiềm chế nhập siêu" đang được Bộ Công thương xây dựng (tài liệu được xác định thuộc độ Mật).

Nguyên nhân của việc để xảy ra các vụ lộ BMNN theo dạng trên là do

các cá nhân, tổ chức đã lợi dụng sơ hở trong công tác quản lý, sử dụng BMNN của người có trách nhiệm, nhất là số giảng viên, học viên, cán bộ quản lý trong các trường cao đẳng, đại học, cán bộ trong các viện, trung tâm nghiên cứu nắm giữ BMNN để thu thập, đăng tải trên các website nhằm mục đích thu lợi về kinh tế.

CHƯƠNG 3. KỸ NĂNG PHÒNG, CHỐNG LỘ, MẤT BÍ MẬT NHÀ NƯỚC TRÊN KHÔNG GIAN MẠNG

I. CÁC NGUYÊN TẮC VÀ GIẢI PHÁP ĐẢM BẢO AN NINH, AN TOÀN THÔNG TIN

1. Các nguyên tắc cơ bản đảm bảo an ninh, an toàn thông tin cho người dùng

a. Các nguyên tắc cơ bản áp dụng khi sử dụng các phần mềm

Việc cập nhật phần mềm định kỳ là một biện pháp quan trọng trong công tác đảm bảo an ninh mạng, góp phần phòng ngừa và ngăn chặn các hành vi xâm nhập trái phép của tội phạm công nghệ cao. Nhiều đối tượng tấn công mạng đã lợi dụng lỗ hổng bảo mật từ các phần mềm cũ để xâm nhập hệ thống, đánh cắp dữ liệu hoặc thực hiện hành vi phá hoại. Những lỗ hổng này chỉ có thể được khắc phục thông qua các bản cập nhật bảo mật từ nhà phát triển.

Phần mềm hiện diện trên nhiều nền tảng, từ hệ điều hành Windows, macOS trên máy tính cá nhân, đến Android, iOS trên thiết bị di động, thậm chí cả các thiết bị mạng như bộ định tuyến và hệ thống nhà thông minh. Do đó, để đảm bảo an toàn thông tin, người dùng cần thường xuyên kiểm tra cập nhật phần mềm và cài đặt ngay khi có phiên bản mới nhằm giảm thiểu rủi ro bị tấn công mạng.

Trong một số trường hợp, các bản cập nhật có thể được cài đặt tự động, giúp hạn chế nguy cơ bị tấn công mạng do sử dụng phần mềm lỗi thời. Các hệ điều hành như Windows, macOS và trình duyệt Google Chrome, Firefox.. đã tích hợp tính năng cập nhật tự động để đảm bảo người dùng luôn sử dụng phiên bản mới nhất với các bản vá bảo mật quan trọng.

Bên cạnh việc cập nhật hệ điều hành, cần chú trọng đến các phần mềm và ứng dụng thường xuyên sử dụng trên máy tính, đặc biệt là các phần mềm liên quan đến truy cập Internet và xử lý dữ liệu như trình duyệt Web, phần mềm đọc PDF, Microsoft Office,... Đây là những phần mềm dễ bị tin tặc khai thác nếu không được cập nhật kịp thời, tiềm ẩn nguy cơ mất an toàn thông tin và rò rỉ dữ liệu quan trọng.

b. Các nguyên tắc áp dụng áp dụng khi sử dụng, cấu hình quản lý mật khẩu

Trong thời đại số, hầu hết người dùng đều cần tạo tài khoản để sử dụng các dịch vụ trực tuyến trên Website và ứng dụng. Việc truy cập các tài khoản này đòi hỏi phải có mật khẩu, tuy nhiên, nhiều người gặp khó khăn trong việc ghi nhớ

nhiều mật khẩu khác nhau. Do đó, họ có xu hướng sử dụng cùng một mật khẩu cho nhiều tài khoản, điều này tiềm ẩn nguy cơ mất an toàn thông tin.

Việc dùng chung mật khẩu có thể khiến tài khoản cá nhân bị xâm phạm nghiêm trọng. Nếu tội phạm mạng chiếm được mật khẩu từ một trang Web hoặc ứng dụng, chúng có thể dễ dàng xâm nhập vào các tài khoản quan trọng khác như tài khoản ngân hàng, Email... gây thiệt hại lớn về tài chính và dữ liệu.

Người dùng cần đặt mật khẩu khác nhau cho từng Website, ứng dụng và dịch vụ. Việc chỉ thay đổi một chữ số hoặc một ký tự không đủ để bảo vệ tài khoản, vì những biến thể này rất dễ bị đoán ra. Để tăng cường bảo mật, nên sử dụng các phần mềm quản lý mật khẩu (Password Managers), giúp tạo và lưu trữ mật khẩu mạnh, giảm nguy cơ bị tấn công và rò rỉ thông tin cá nhân.

Phần mềm quản lý mật khẩu:

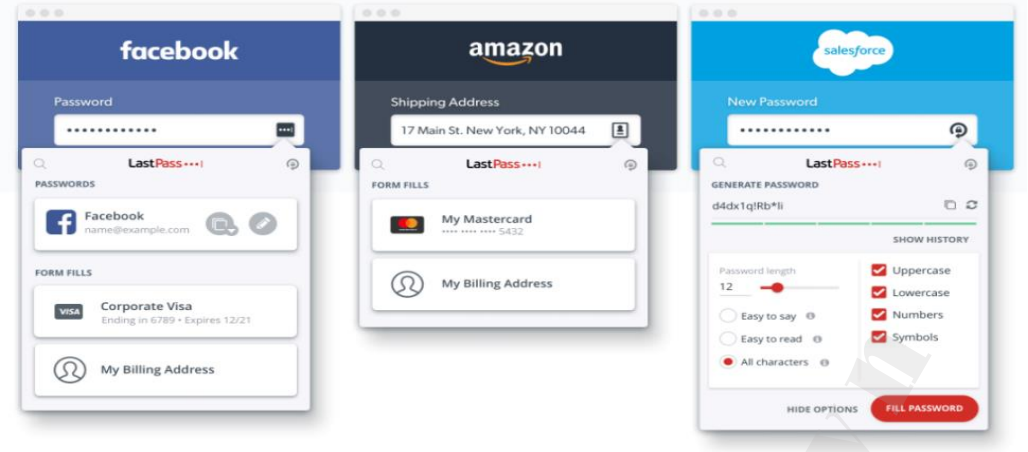
Một phần mềm quản lý tất cả các password trong một kho kỹ thuật số có khóa bảo vệ và đảm bảo an toàn cho chúng bằng một password mạnh là password chính duy nhất. Bằng cách này, chỉ phải nhớ một password để truy cập tất cả tài khoản. Những ứng dụng này có thể dễ dàng sinh ra các password phức tạp, như *6ur7qvsZpb0ZkcuSW1u!V8ng!L^lb*. Một password như vậy không thể đoán được và vô cùng khó/không khả thi để bẻ khóa trong thời gian hữu hạn.

Các phần mềm quản lý password có thể tự động điền thông tin đăng nhập khi truy cập một Website người dùng đã từng sử dụng và có password được lưu. Chỉ riêng chức năng đã giúp bảo vệ khỏi rất nhiều các tấn công. Nếu như địa chỉ Website không chính xác, ví dụ: *vidu.mybanklogin.com*, ứng dụng quản lý password sẽ không điền thông tin đăng nhập website ngân hàng *vidu* vào. Cũng có thể sử dụng một ứng dụng quản lý password để lưu trữ các ghi chú (note), ví dụ các mã đăng nhập, các khóa bí mật và câu trả lời cho các câu hỏi bí mật.

Một số ứng dụng quản lý password tốt: LastPass, 1Password, Bitwarden và KeePass.

LastPass: là ứng dụng quản lý mật khẩu có rất nhiều chức năng, bao gồm một ứng dụng mở rộng cho trình duyệt web để sinh mật khẩu ngẫu nhiên và điền thông tin đăng nhập cho người dùng.

- LastPass có các ứng dụng tốt cho các hệ điều hành cơ bản thường gặp và vẫn hoạt động tốt ngay cả với phiên bản miễn phí. Phiên bản có phí cho một gigabyte để lưu trữ tài liệu nhạy cảm và lựa chọn để chia sẻ (share) password với những người dùng LastPass khác.



Hình 1. Phần mềm LastPass

1Password: nổi tiếng với thiết kế đẹp và được tối ưu cho việc sử dụng trên các thiết bị của Apple, như iPhone và Macbook. Ứng dụng này có một ứng dụng mở rộng trình duyệt (extension) 1Password X cho phép sinh ra các password ngẫu nhiên và điền chúng vào khi người dùng truy cập các website. Khi đăng ký dịch vụ của 1Password, người dùng sẽ nhận được một khóa bảo mật đặc biệt (khóa bí mật), người dùng cần dùng khóa này và Master Password để có thể truy cập tài khoản .

Bitwarden: đã trở nên khá thông dụng những năm gần đây. Đây là 1 ứng dụng hoàn toàn mở, có thể cài đặt trên nhiều nền tảng và có thể sử dụng miễn phí. Người dùng có thể chia sẻ password, một chức năng mà người dùng phải trả phí để sử dụng trong hầu hết các ứng dụng quản lý password khác. Nếu người dùng muốn chia sẻ password với nhiều người, ứng dụng sẽ thu phí 1 USD một tháng, đồng thời dịch vụ cũng sẽ cung cấp 1 gigabyte chứa dữ liệu cho các file . Những người dùng rành kỹ thuật có thể tự vận hành hạ tầng Bitwarden cho riêng mình.

KeePass: được xem là ứng dụng quản lý password an toàn nhất, bởi vì nhiều chuyên gia bảo mật sử dụng ứng dụng này và đã tham gia làm cho nó an toàn hơn với kiến thức chuyên môn của họ.

Điểm hạn chế là ứng dụng này nhìn khá cũ (old-fashioned), giống như một ứng dụng Windows XP. Tuy nhiên, cộng đồng sử dụng KeePass có nhiều lập trình viên đầy đam mê đã làm những ứng dụng đẹp hơn với KeePass, ví dụ MacPass for MacOS. Một lựa chọn tốt khác là KeePassXC, về nhiều mặt là một phiên bản tốt và đầy đủ hơn cho KeePass, và cũng thường xuyên được cập nhật bởi một nhóm các lập trình viên đầy nhiệt huyết.

Mật khẩu mạnh

Các Website và ứng dụng thường yêu cầu sử dụng mật khẩu có chữ và số.

Nhưng một password như thế nào là 1 password mạnh? Nhiều người nghĩ P@ssword007 là 1 password mạnh nhưng trong thực tế, password này khá dễ crack đối với các hacker. Đó là lý do tại sao nên cân nhắc sử dụng passphrase (cụm password) thay vì các password được tạo với 1 từ đơn giản.

Cụm password dài nhưng dễ nhớ, là 2 điều kiện tiên quyết cho một password mạnh. Một passphrase như ***I eat 2 whole pizzas every week*** thì dễ nhớ và khá khó để để crack. Ngoài ra, cũng nên sử dụng các khoảng trắng trong các password; đây là 1 lựa chọn mà chúng ta thường bỏ qua.

Cũng có thể tạo một password bằng cách đặt những từ ngẫu nhiên lại với nhau với phương pháp **Diceware** với 1 **Wordlist** tốt đủ lớn. Diceware hiện tại gần như là phương pháp an toàn nhất để tạo một password mà người dùng có thể nhớ được.

Tóm lại, cách tốt nhất để lưu trữ password:

+ Sử dụng một phần mềm quản lý password (password manager), nên là 1 trong các phần mềm được giới thiệu ở trên.

+ Sử dụng một passphrase hoặc phương pháp Diceware để tạo password.

+ Viết xuống password quản lý mật khẩu (master password/manager password để đăng nhập password manager) và giữ nó ở một nơi an toàn, đảm bảo rằng không bao giờ mất khả năng truy cập password manager.

Sử dụng password manager để sinh ra các password có độ dài từ 20 ký tự trở lên và để password manager lưu trữ những password này.

Những cách thức lưu giữ password an toàn khác

iCloud Keychain*:* là 1 cách lưu trữ password nếu người dùng chỉ tập trung sử dụng các sản phẩm của Apple. Keychain có thể sinh password và tự động điền password. Chức năng của iCloud Keychain khá là giới hạn so với các ứng dụng quản lý password khác. Nếu sử dụng iCloud Keychain ít nhất người dùng cần sử dụng một password mạnh và xác thực 2 yếu tố (đa nhân tố) cho tài khoản iCloud.

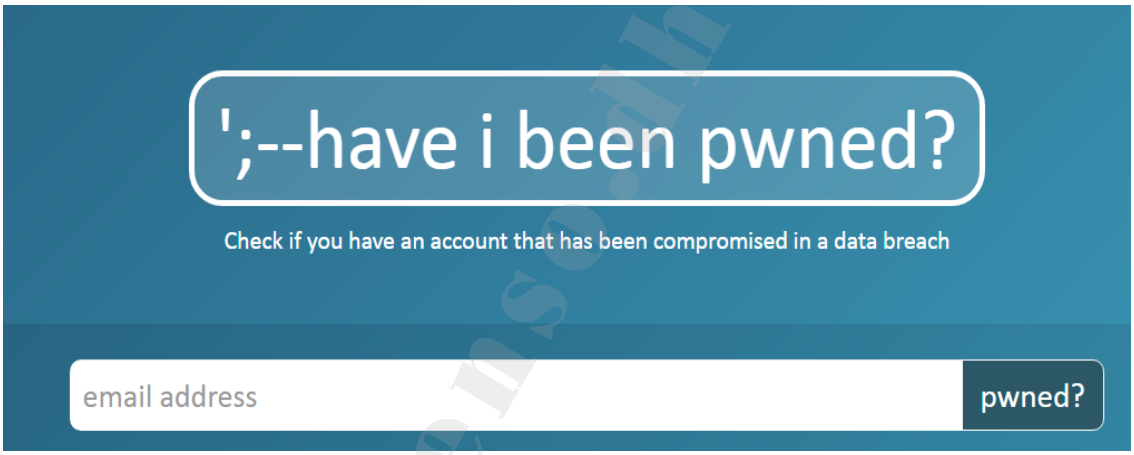
Lưu trong trình duyệt*:* Các trình duyệt như Chrome và Firefox cho phép lưu password trong trình duyệt nhưng sử dụng một ứng dụng quản lý password là 1 lựa chọn tốt hơn.

Sổ tay password*:* Giấy và bút có thể được dùng để lưu giữ password. Hãy đảm bảo rằng các password duy nhất khác nhau và lưu trữ chúng cẩn thận. Và luôn nhớ tạo ra một bản copy làm backup.

Nếu lo lắng người khác có thể đọc được password ghi trên giấy của mình, hãy chú ý không để mọi người có thể tiếp cận đến sổ tay. Một thủ thuật hữu dụng nữa là có thể thêm một từ cố định vào password (không ghi ra từ này vào sổ tay password, chỉ đơn giản là nhớ nó). Nếu ai đó có thể tiếp cận sổ tay password, ít nhất họ không thể sử dụng password đã viết ra, bởi vì chúng đã thiếu mất một thành phần quan trọng đã được nhớ bằng não.

Cập nhật danh sách những password đã bị đánh cắp

Dù cho password có mạnh đến đâu đi nữa, nó cũng có thể bị đánh cắp. Chính vì vậy, cần kiểm tra xem các password đã bị đánh cắp bởi các hacker chưa. Có thể sử dụng website ***Have I Been Pwned*** hỗ trợ theo dõi các Website đã bị hack mà tài khoản bị ảnh hưởng và sẽ cảnh báo khi có thông tin xuất hiện. Nên thường xuyên làm việc kiểm tra này để giữ an toàn cho tài khoản.



Hình 2. Website: Have I Been Pwned

Nếu đăng ký với website *Have I Been Pwned*, người dùng sẽ nhận được thông báo mỗi khi hệ thống website này phát hiện email nằm trong danh sách các file chứa thông tin tài khoản bị đánh cắp. Bằng cách này, sẽ biết chính xác những password nào đã bị đánh cắp trong các sự cố đó, dựa vào thông tin dịch vụ hay website đã bị hacker xâm nhập. Nếu *Have I Been Pwned* tìm thấy email nằm trong các file bị đánh cắp, người dùng nên thay đổi ngay password tương ứng.

Xác thực Hai Yếu Tố (Đa Nhân Tố)

Để giới hạn làm giảm mức độ ảnh hưởng khi một password bị đánh cắp, nên sử dụng xác thực 2 yếu tố (2FA, đa nhân tố) là một phương pháp bảo mật hiện đại. Có thể kích hoạt xác thực 2 yếu tố qua các dịch vụ sử dụng, nếu như dịch vụ đó hỗ trợ xác thực 2 yếu tố. Sau khi đăng nhập với username và password, kể từ bây giờ sẽ phải thực hiện thêm một bước thứ 2 khi đăng nhập. Thông thường, dịch vụ của website sẽ yêu cầu nhập vào mã được sinh cho người dùng

qua một smartphone (điện thoại thông minh) bằng các ứng dụng authentication hoặc tin nhắn từ dịch vụ.

Nếu một hacker tìm cách có được thông tin đăng nhập, người đó sẽ cần phải lấy được cả mã đăng nhập được tạo ra cho điện thoại ngay khi hacker thử đăng nhập tài khoản. Việc này tạo khó khăn cho hacker vì chúng cần truy cập điện thoại hoặc đánh cắp mã xác thực được gửi đến điện thoại.

Xác thực hai yếu tố cũng cảnh báo cho người dùng những cố gắng truy cập thâm nhập tài khoản, trong trường hợp password bị đánh cắp và người dùng nhận được thông báo của dịch vụ website về việc có người cố gắng truy cập tài khoản với password. Nhờ vậy, người dùng sẽ biết được có ai đó đã cố gắng xâm nhập tài khoản.

Sử dụng website *Two Factor Auth List* để kiểm tra các dịch vụ, ứng dụng, website nào đã hỗ trợ xác thực hai yếu tố (đa nhân tố). Google, Apple, Facebook, Instagram, WhatsApp và Dropbox đều đã là các dịch vụ hỗ trợ các chức năng xác thực hai yếu tố (đa nhân tố).

+ Mã xác thực qua tin nhắn điện thoại

Nhận mã xác thực qua tin nhắn điện thoại rất đơn giản: người dùng link số điện thoại vào một dịch vụ online và điền mã xác thực được gửi đến điện thoại tương ứng với website hay app đó. Chú ý là các hacker có thể lấy được các mã xác thực đăng nhập bằng cách can thiệp vào quá trình nhận tin nhắn điện thoại hoặc sử dụng những kỹ thuật lừa đảo. Vì vậy, nhiều chuyên gia đã khuyến nghị không sử dụng xác thực 2 yếu tố qua tin nhắn điện thoại mà thay thế bằng phương thức xác thực 2 yếu tố khác an toàn hơn như sử dụng "mã xác thực qua các ứng dụng Authenticator" của Google chẳng hạn.

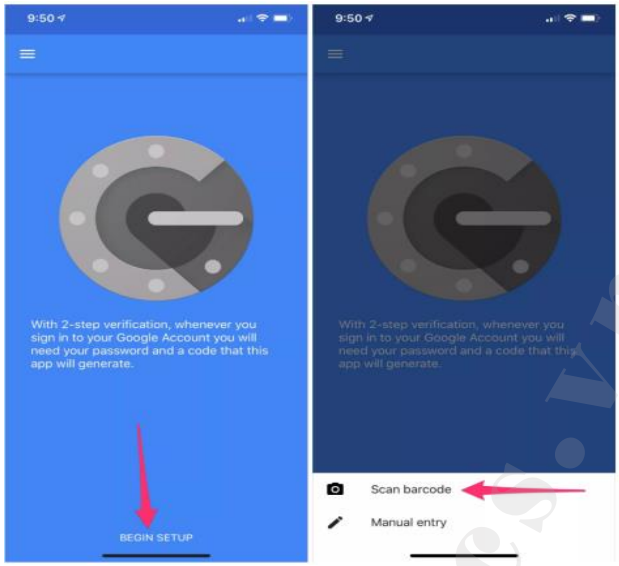
+ Mã xác thực qua các ứng dụng authenticator

Một cách an toàn cho xác thực hai yếu tố là sử dụng một ứng dụng authenticator. Những ứng dụng này cho phép người dùng scan một QR-code là một barcode để scan bằng camera của smartphone.

Mã QR-code được cung cấp bởi dịch vụ mà người dùng muốn bảo mật. Sau khi scan QR-code, một mã bảo mật sẽ xuất hiện trên màn hình trong vòng 30 giây, ngay sau đó một mã khác sẽ được sinh ra.

Những mã ngẫu nhiên này cho phép người dùng xác thực việc truy cập , để dịch vụ online biết rằng người dùng chính là người đang cố gắng truy cập tài khoản. 1Password, LastPass Authenticator, Authy và Google Authenticator đều

sinh ra các mã như vậy.



Hình 3. Xác thực qua ứng dụng Authenticator

Chú ý rằng khi sử dụng Google Authenticator, nếu người dùng để mất điện thoại hoặc nếu ứng dụng Google Authenticator bị reset, người dùng sẽ mất tất cả các mã xác thực đăng nhập trên điện thoại đó. Những ứng dụng authenticator khác được nhắc ở trên cho phép người dùng đồng bộ các mã xác thực đăng nhập này trên tất cả các thiết bị mà người dùng sử dụng ứng dụng đó.

c. Các nguyên tắc khi sao lưu dữ liệu

- Sao lưu (backup) là một giải pháp thiết yếu giúp bảo vệ dữ liệu quan trọng khỏi các sự cố bất ngờ. Nếu máy tính đột ngột hỏng hóc, dữ liệu trên thiết bị có thể bị mất vĩnh viễn. Việc xác định những hình ảnh, video, tài liệu quan trọng phục vụ công việc và cá nhân là bước cần thiết để đảm bảo những dữ liệu này được sao lưu kịp thời.

- Backup không chỉ giúp bảo vệ dữ liệu khi thiết bị gặp sự cố phần cứng, mà còn là lớp phòng vệ trước các rủi ro như mất trộm điện thoại, tấn công ransomware khiến hệ thống bị khóa hoặc không thể truy cập. Một bản sao lưu đầy đủ và định kỳ sẽ giúp người dùng nhanh chóng khôi phục công việc, giảm thiểu tổn thất do mất dữ liệu.

- Để tăng cường an toàn thông tin, nên thực hiện sao lưu theo nguyên tắc **3-2-1:** giữ ít nhất **ba bản sao dữ liệu**, lưu trữ trên hai loại thiết bị khác nhau (như ổ cứng ngoài, dịch vụ lưu trữ đám mây), và có ít nhất một bản sao lưu ngoại tuyến để đảm bảo dữ liệu luôn được bảo vệ trong mọi tình huống.

- Có thể tạo các bản backup online với một dịch vụ cloud như Dropbox,

Degoo, pCloud và những bản backup offline sử dụng ổ cứng rời gắn ngoài. Hãy đảm bảo rằng kiểm tra thường xuyên định kỳ các file được lưu trữ vẫn ở đúng vị trí của chúng và vẫn hoạt động tốt.

d. Nguyên tắc sử dụng trình duyệt truy cập Internet an toàn

- Kiểm tra biểu tượng ổ khóa (và các yếu tố khác)

Biểu tượng ổ khóa trên thanh địa chỉ của trình duyệt là dấu hiệu cho thấy kết nối giữa thiết bị của người dùng và website đang được mã hóa. Điều này giúp bảo vệ dữ liệu cá nhân, như mật khẩu hay thông tin thẻ tín dụng, khỏi nguy cơ bị tội phạm mạng đánh cắp trong quá trình truyền tải.

Để đảm bảo an toàn, người dùng chỉ nên nhập thông tin nhạy cảm trên các website có biểu tượng ổ khóa này. Ngoài ra, địa chỉ website bắt đầu bằng "https://" cho thấy trang web sử dụng giao thức bảo mật SSL/TLS, giúp tăng cường tính bảo mật và giảm nguy cơ bị tấn công đánh cắp dữ liệu.

Tuy nhiên, dù một trang web có "https://", điều đó không đảm bảo tuyệt đối rằng trang web đó là hợp pháp. Tội phạm mạng có thể tạo ra các trang web giả mạo với giao thức mã hóa nhằm đánh lừa người dùng. Do đó, cần kiểm tra kỹ địa chỉ website, tránh truy cập các liên kết đáng ngờ và sử dụng các công cụ bảo mật để tăng cường bảo vệ thông tin cá nhân.

Hình 4. Kiểm tra địa chỉ trang web

Hãy chú ý đặc biệt vào địa chỉ website và kiểm tra rằng địa chỉ đó có chính xác hay không.

Ví dụ:

Chính xác: *https://www.facebook.com* (facebook.com là tên miền chính)

Sai: *https://www.facebook.tech* (.tech không phải là phần mở rộng tên miền đúng)

Sai: *https://facebook.login.net* (login.net là tên miền chính ở đây)

Sai: *https://www.faceb00k.com* (2 chữ o đã được thay thế bằng 2 chữ số 0)

2. Các giải pháp đảm bảo an ninh, an toàn thông tin cho máy tính

a. Giải pháp cơ bản khi cài đặt cấu hình máy tính an toàn

- Kích hoạt tự động cập nhật

Như người dùng đã có thể đoán trước: việc cập nhật cho các thiết bị rất quan trọng. Đó là lý do vì sao chúng tôi khuyến nghị hãy để các bản cập nhật cho máy tính được tự động cài đặt. Windows và MacOS hỗ trợ chức năng này, Google Chrome cũng hỗ trợ chức năng tương tự.

Nếu phần mềm người dùng dùng không hỗ trợ chức năng tự động cập nhật hay thông báo các bản cập nhật mới, hãy kiểm tra tính khả tín của thông báo có bản cập nhật này trước tiên. Các virus thường lây lan qua các thông báo, cảnh báo giả, ví dụ như là một bản update cho Adobe Flash Player. Những cảnh báo này thường xuất hiện nhan nhản khi người dùng duyệt web. Nếu như người dùng muốn đảm bảo rằng thông báo đó có thể tin tưởng được, người dùng hãy vào chính phần mềm đó và kiểm tra thủ công xem liệu đã có một bản cập nhật hay chưa.

- Cài đặt lại máy tính định kỳ

Để duy trì hiệu suất và bảo mật cho máy tính, người dùng nên thực hiện cài đặt lại hệ điều hành sau mỗi ba năm. Quá trình này bao gồm sao lưu dữ liệu quan trọng, xóa hoàn toàn ổ cứng, và cài đặt lại hệ điều hành (Windows, macOS).

Việc cài đặt lại hệ thống giúp:

+ Tăng tốc máy tính: Loại bỏ các tệp rác, phần mềm không cần thiết tích tụ theo thời gian.

+ Xóa bỏ phần mềm độc hại: Giảm nguy cơ bị tấn công bởi virus hoặc phần mềm gián điệp.

+ Tạo môi trường hệ thống sạch sẽ: Đảm bảo chỉ có những ứng dụng cần thiết được cài đặt lại, giúp máy hoạt động ổn định hơn.

Để quá trình diễn ra an toàn, hãy chắc chắn rằng:

+ Sao lưu dữ liệu quan trọng trước khi xóa ổ cứng.

+ Tải xuống phiên bản hệ điều hành mới nhất từ nguồn chính thức.

+ Cài đặt lại phần mềm cần thiết và tránh cài đặt những ứng dụng không rõ nguồn gốc.

Việc cài đặt lại máy tính theo chu kỳ không chỉ giúp duy trì hiệu suất tối

ưu mà còn góp phần nâng cao bảo mật, giảm nguy cơ bị tấn công bởi mã độc.

b. Các giải pháp an toàn dữ liệu trên máy tính

- Các thiết bị ổ cứng di động và thiết bị thông minh

Trong công tác bảo vệ dữ liệu, một phương thức tấn công phổ biến của tội phạm mạng là cài cắm mã độc vào thiết bị lưu trữ di động (USB, ổ cứng di động, thẻ nhớ…) và tìm cách để cán bộ, chiến sĩ vô tình kết nối thiết bị này vào hệ thống máy tính của đơn vị. Khi đó, mã độc có thể lây lan, đánh cắp thông tin hoặc phá hoại dữ liệu quan trọng. Vì vậy, tuyệt đối không sử dụng các thiết bị lưu trữ không rõ nguồn gốc, dù là nhặt được hay được tặng. Nếu bắt buộc phải kiểm tra thiết bị, hãy chuyển cho bộ phận an ninh mạng hoặc chuyên gia kỹ thuật để kiểm tra trước khi sử dụng.

Bên cạnh đó, cần cân nhắc kỹ trước khi sử dụng các thiết bị thông minh có kết nối Internet. Những thiết bị như camera giám sát, máy in, router WiFi, thậm chí cả thiết bị gia dụng thông minh có thể trở thành điểm yếu để đối tượng xấu xâm nhập hệ thống mạng nội bộ. Tội phạm mạng có thể lợi dụng các lỗ hổng bảo mật để kiểm soát, theo dõi và đánh cắp thông tin từ những thiết bị này. Vì vậy, chỉ sử dụng các thiết bị thực sự cần thiết, ưu tiên các sản phẩm có chứng nhận bảo mật cao và do các hãng uy tín cung cấp. Đồng thời, thường xuyên cập nhật phần mềm, thay đổi mật khẩu mặc định và áp dụng các biện pháp bảo mật nghiêm ngặt để hạn chế rủi ro an ninh.

- Xóa các tập tin

Việc xóa dữ liệu thông thường bằng cách nhấn Delete hoặc dọn dẹp thùng rác không đảm bảo rằng dữ liệu đó đã bị loại bỏ hoàn toàn. Các tập tin vẫn có thể được khôi phục bằng các phần mềm phục hồi dữ liệu, gây nguy cơ rò rỉ thông tin mật. Vì vậy, khi xử lý các tập tin quan trọng, cán bộ, chiến sĩ cần sử dụng các công cụ xóa dữ liệu chuyên dụng để đảm bảo dữ liệu không thể khôi phục được.

Xóa dữ liệu trên Windows

Sử dụng phần mềm BleachBit, một công cụ mã nguồn mở, để xóa hoàn toàn dữ liệu trên ổ cứng. BleachBit có thể:

+ Ghi đè lên các tập tin đã bị xóa nhiều lần bằng thuật toán an toàn.

+ Xóa sạch bộ nhớ đệm, file tạm, lịch sử duyệt web và các dấu vết còn sót lại.

+ Hỗ trợ xóa dữ liệu theo tiêu chuẩn DoD 5220.22-M (chuẩn xóa dữ liệu của Bộ Quốc phòng Mỹ).

Hướng dẫn xóa dữ liệu an toàn bằng BleachBit trên Windows:

+ Tải và cài đặt BleachBit từ trang chính thức.

+ Chạy ứng dụng, chọn chế độ "Shred Files" hoặc "Wipe Free Space" để ghi đè lên dữ liệu cần xóa.

+ Xác nhận và tiến hành xóa dữ liệu vĩnh viễn.

Xóa dữ liệu trên macOS

Mặc dù BleachBit có thể hoạt động trên macOS với một số tinh chỉnh, nhưng Permanent Eraser là giải pháp tối ưu hơn. Ứng dụng này sử dụng thuật toán 35-pass Gutmann – một trong những phương pháp xóa dữ liệu an toàn nhất hiện nay.

Hướng dẫn xóa dữ liệu an toàn bằng Permanent Eraser trên macOS:

+ Tải và cài đặt Permanent Eraser.

+ Kéo và thả các tập tin vào ứng dụng để xóa vĩnh viễn.

+ Chờ quá trình xóa hoàn tất, đảm bảo dữ liệu không thể khôi phục được.

+ Xóa dữ liệu trên thiết bị lưu trữ ngoài (USB, ổ cứng di động, SSD)

+ Đối với ổ HDD: Sử dụng BleachBit hoặc các công cụ như Eraser (Windows) hoặc Secure Empty Trash (macOS).

+ Đối với ổ SSD: Kích hoạt lệnh ATA Secure Erase hoặc sử dụng phần mềm của nhà sản xuất (Samsung Magician, Crucial Storage Executive…).

+ Đối với USB, thẻ nhớ: Format theo phương pháp Full Format và ghi đè dữ liệu nhiều lần bằng BleachBit hoặc Permanent Eraser.

c. Một số giải pháp khi sử dụng trình duyệt web, ứng dụng

- Sử dụng Google Chrome với 3 ứng dụng mở rộng trình duyệt sau:

Hiện nay, Google Chrome được đánh giá là một trong những trình duyệt an toàn và thân thiện nhất với người dùng. Ngoài ra, Firefox, Safari, và Microsoft Edge cũng là những lựa chọn tốt. Tuy nhiên, không nên sử dụng Internet Explorer do trình duyệt này đã lỗi thời và không còn được hỗ trợ cập nhật bảo mật.

Hình 5. Trình duyệt Google Chrome

- Ba tiện ích mở rộng cần thiết để bảo vệ trình duyệt:

+ *uBlock Origin* - Chặn quảng cáo và trình theo dõi

Ứng dụng này giúp ngăn chặn quảng cáo độc hại (malvertising) và các trình theo dõi trực tuyến, bảo vệ quyền riêng tư của người dùng. Không giống như Adblock và Adblock Plus, uBlock Origin không có mô hình kinh doanh đáng ngờ. Nếu muốn hỗ trợ các website yêu thích, người dùng có thể thêm chúng vào danh sách trắng (whitelist) để quảng cáo trên các trang này vẫn hiển thị.

+ *HTTPS Everywhere* - Buộc kết nối an toàn

Tiện ích này tự động chuyển hướng người dùng đến các phiên bản HTTPS của website nếu có, giúp mã hóa dữ liệu và ngăn chặn các cuộc tấn công trung gian (Man-in-the-Middle). Nếu hacker cố gắng chuyển hướng người dùng đến một kết nối không an toàn, HTTPS Everywhere sẽ chặn hành vi này.

+ *PDF Viewer* - Đọc file PDF an toàn

Tội phạm mạng thường giấu mã độc trong các file PDF nhằm khai thác lỗ hổng bảo mật của Adobe Reader. Thay vì mở file bằng phần mềm này, người dùng nên sử dụng PDF Viewer để mở trực tiếp trong trình duyệt, giúp giảm nguy cơ bị tấn công. Firefox cũng hỗ trợ mở PDF ngay trong trình duyệt mà không cần cài thêm phần mềm.

Cài đặt ba tiện ích mở rộng này sẽ giúp trình duyệt an toàn hơn, bảo vệ người dùng khỏi quảng cáo độc hại, lừa đảo trực tuyến và các cuộc tấn công mạng phổ biến.

- Tắt JavaScript và các macro, kích hoạt ứng dụng tường lửa (firewall)

Tội phạm mạng thường khai thác các tính năng đặc biệt trong phần mềm để cài mã độc vào máy tính. Do đó, để tăng cường bảo mật, người dùng nên vô hiệu hóa các chức năng không cần thiết, cụ thể là:

+ *Tắt JavaScript trong Adobe Reader*: Hạn chế nguy cơ bị khai thác thông qua lỗ hổng bảo mật trong các tài liệu PDF chứa mã độc.

+ *Tắt Macro trong Microsoft Office*: Giúp ngăn chặn mã độc từ các tệp Word, Excel có chứa macro nguy hiểm.

Bên cạnh việc vô hiệu hóa các tính năng dễ bị tấn công, người dùng cần bật tường lửa (firewall) để bảo vệ thiết bị khỏi các cuộc tấn công mạng từ bên ngoài:

+ *Trên macOS*: Bật firewall trong System Preferences → Security & Privacy → Firewall. Nếu muốn tăng cường giám sát, có thể sử dụng Little Snitch, một ứng dụng theo dõi các kết nối Internet của phần mềm đang chạy trên hệ thống.

+ *Trên Windows*: Tường lửa Windows Defender thường được bật mặc định nếu hệ điều hành là phiên bản có bản quyền. Nếu cần giám sát sâu hơn các kết nối mạng, người dùng có thể sử dụng GlassWire.

+ *Trên router*: Nếu router có hỗ trợ firewall, hãy bật tính năng này để ngăn chặn các truy cập trái phép ngay từ lớp mạng.

- Tránh sử dụng Flash để bảo vệ thiết bị khỏi rủi ro bảo mật

Adobe Flash từng là công nghệ phổ biến để hiển thị video, game và nội dung tương tác trên trình duyệt. Tuy nhiên, Flash đã lỗi thời và tiềm ẩn nhiều nguy cơ bảo mật, khiến nó trở thành mục tiêu khai thác của tội phạm mạng.

Không nên cài đặt hoặc sử dụng Flash trên máy tính. Hầu hết trình duyệt đã mặc định vô hiệu hóa Flash và yêu cầu người dùng kích hoạt thủ công nếu thực sự cần thiết. Chỉ kích hoạt Flash trên các website hoàn toàn tin cậy, và chỉ khi có yêu cầu đặc biệt.

Hiện nay, hầu hết các website đã chuyển sang công nghệ hiện đại như HTML5, giúp hiển thị video, game và nội dung tương tác một cách an toàn hơn mà không cần Flash.

Adobe đã ngừng hỗ trợ Flash từ năm 2020 và khuyến nghị tất cả người dùng gỡ bỏ hoàn toàn Flash để tránh rủi ro bảo mật. Vì vậy, nếu máy tính vẫn

còn cài đặt Flash, hãy gỡ bỏ ngay lập tức để bảo vệ thiết bị khỏi các cuộc tấn công mạng.

- Chú ý các Certificate (chứng chỉ số) để ngăn chặn theo dõi trái phép

Tội phạm mạng có thể sử dụng chứng chỉ số (certificate) giả mạo để theo dõi hoạt động của người dùng, ngay cả khi họ đang duyệt web qua kết nối HTTPS. Khi một chứng chỉ độc hại được cài vào máy tính hoặc thiết bị di động, hacker có thể chặn và đọc toàn bộ dữ liệu mà người dùng gửi đi trên Internet, bao gồm thông tin cá nhân, mật khẩu và dữ liệu tài chính.

+ Thủ đoạn phổ biến:

Nạn nhân thường bị lừa cài đặt một chứng chỉ khi cố gắng truy cập mạng WiFi công cộng hoặc một dịch vụ trực tuyến. Hacker có thể yêu cầu người dùng tải và cài chứng chỉ để "hỗ trợ kết nối", nhưng thực chất đây là một hành vi tấn công nhằm giám sát và đánh cắp thông tin.

+ Biện pháp phòng tránh:

- Không bao giờ cài đặt chứng chỉ chỉ để truy cập Internet, đặc biệt trên WiFi công cộng.
- Nếu có yêu cầu cài chứng chỉ, hãy xác minh với quản trị viên mạng để đảm bảo đó là yêu cầu chính thống.
- Kiểm tra danh sách các chứng chỉ đã cài đặt trên thiết bị và xóa ngay lập tức những chứng chỉ đáng ngờ.
- Sử dụng VPN đáng tin cậy để mã hóa lưu lượng truy cập và bảo vệ quyền riêng tư khi sử dụng mạng WiFi công cộng.
- Luôn cảnh giác khi có yêu cầu cài đặt chứng chỉ số. Nếu không chắc chắn, tuyệt đối không cài đặt để tránh bị giám sát và đánh cắp thông tin cá nhân.

d. Giải pháp mã hóa ổ cứng và sao lưu dữ liệu

Để bảo vệ dữ liệu quan trọng, việc mã hóa ổ cứng và các bản sao lưu (backup) là một yêu cầu bắt buộc. Mã hóa giúp đảm bảo rằng ngay cả khi thiết bị bị mất, đánh cắp hoặc rơi vào tay đối tượng xấu, dữ liệu vẫn không thể bị truy cập nếu không có khóa giải mã hợp lệ.

- Mã hóa ổ cứng trên macOS

Apple cung cấp công cụ mã hóa tích hợp FileVault giúp bảo vệ toàn bộ dữ liệu trên MacBook và iMac chỉ với một thao tác đơn giản.

Cách kích hoạt FileVault trên macOS:

+ Mở System Settings (Cài đặt hệ thống) > Privacy & Security (Quyền riêng tư & Bảo mật).

+ Chọn FileVault và bật tính năng này.

+ Lưu trữ khóa khôi phục ở nơi an toàn (tránh lưu trực tiếp trên máy tính).

+ Sau khi kích hoạt, tất cả dữ liệu trên ổ đĩa sẽ được mã hóa, đảm bảo rằng ngay cả khi thiết bị bị đánh cắp, đối tượng cũng không thể truy cập vào dữ liệu bên trong.

- Mã hóa ổ cứng trên Windows

Sử dụng BitLocker (Windows Pro & Enterprise)

Windows cung cấp công cụ mã hóa BitLocker, nhưng chỉ có sẵn trên các phiên bản Windows Pro và Enterprise. Nếu hệ thống sử dụng phiên bản này, hãy kích hoạt ngay BitLocker để bảo vệ ổ cứng.

Cách kích hoạt BitLocker trên Windows:

+ Mở Control Panel > BitLocker Drive Encryption.

+ Chọn ổ đĩa cần mã hóa và nhấn Turn on BitLocker.

+ Chọn phương thức lưu trữ khóa khôi phục (USB, Microsoft account, in ra giấy…).

+ Xác nhận và chờ quá trình mã hóa hoàn tất.

Sử dụng VeraCrypt (Windows Home và các hệ thống khác)

Nếu máy tính không hỗ trợ BitLocker, VeraCrypt là một lựa chọn thay thế an toàn và đáng tin cậy. Đây là phần mềm mã hóa mã nguồn mở, được sử dụng rộng rãi trong lĩnh vực bảo mật. Cách sử dụng VeraCrypt để mã hóa ổ cứng:

Tải và cài đặt VeraCrypt từ trang chính thức.

+ Mở ứng dụng, chọn System > Encrypt System Partition/Drive.

+ Chọn Normal Mode hoặc Hidden Mode để mã hóa (tùy vào nhu cầu bảo mật).

+ Tạo mật khẩu mạnh và lưu trữ khóa khôi phục ở nơi an toàn.

+ Tiến hành mã hóa (có thể mất từ vài giờ đến vài ngày tùy vào dung lượng ổ cứng).

Lưu ý: Trước khi mã hóa, cần backup (sao lưu) dữ liệu quan trọng để tránh

mất mát nếu xảy ra sự cố trong quá trình mã hóa.

- Mã hóa dữ liệu backup

Không chỉ ổ cứng chính, các bản sao lưu (backup) cũng cần được mã hóa để ngăn chặn rò rỉ thông tin.

+ Backup trên macOS: Dùng Time Machine kết hợp với FileVault hoặc sử dụng VeraCrypt để tạo ổ đĩa ảo được mã hóa.

+ Backup trên Windows: Dùng BitLocker để mã hóa ổ cứng ngoài hoặc sử dụng VeraCrypt để mã hóa từng file/folder quan trọng.

+ Backup trên USB/ổ cứng di động: Nên sử dụng VeraCrypt hoặc BitLocker To Go để mã hóa thiết bị lưu trữ di động.

- Lưu trữ và quản lý khóa mã hóa

Việc bảo vệ khóa mã hóa rất quan trọng, nếu mất khóa, dữ liệu sẽ không thể phục hồi. Một số phương án lưu trữ an toàn:

+ Lưu trữ trong USB bảo mật chuyên dụng.

+ Viết ra giấy và cất giữ tại nơi an toàn.

+ Sử dụng quản lý mật khẩu như Bitwarden hoặc KeePass để lưu khóa mã hóa.

Việc mã hóa ổ cứng và backup dữ liệu là biện pháp quan trọng để bảo vệ thông tin quan trọng của cá nhân và tổ chức, giúp ngăn chặn rò rỉ và đảm bảo an toàn dữ liệu ngay cả trong trường hợp thiết bị bị mất hoặc đánh cắp.

3. Các nguyên tắc đảm bảo an ninh, an toàn thông tin áp dụng cho điện thoại thông minh và máy tính bảng

a. Một số phương thức tấn công

Sự phát triển nhanh chóng của công nghệ đã biến điện thoại thông minh trở thành công cụ hỗ trợ đắc lực trong cuộc sống. So với những thiết bị di động đơn giản của thập niên 1980, ngày nay, smartphone giúp người dùng xử lý công việc hiệu quả hơn: kiểm tra email, sử dụng mạng xã hội, đặt phương tiện di chuyển, mua sắm trực tuyến... Tuy nhiên, mức độ tiện lợi này cũng đi kèm với sự gia tăng đáng kể về rủi ro bảo mật.

Điện thoại thông minh ngày càng yêu cầu nhiều quyền truy cập vào dữ liệu cá nhân, tài chính và các thông tin nhạy cảm khác để có thể cung cấp trải nghiệm tốt hơn. Chính điều này đã khiến chúng trở thành mục tiêu tấn công của hacker. Các đối tượng xấu không ngừng tìm cách khai thác lỗ hổng bảo mật trong hệ điều

hành, ứng dụng và cả thói quen sử dụng của người dùng để đánh cắp thông tin.

Dưới đây là một số phương thức tấn công phổ biến mà tội phạm mạng sử dụng để xâm nhập và đánh cắp dữ liệu từ điện thoại di động. Mặc dù nhiều trong số này đã được khắc phục trên các hệ thống hiện đại, nhưng người dùng vẫn cần cảnh giác, đặc biệt là trong môi trường yêu cầu bảo mật cao như ngành công an.

- Bluetooth

Bluetooth là công nghệ không dây tiện lợi giúp kết nối tai nghe, đồng bộ với xe hơi, máy tính và các thiết bị khác. Tuy nhiên, nó cũng là một trong những phương thức bị hacker khai thác để tấn công, đánh cắp thông tin. Đối với ngành công an, nơi dữ liệu cần được bảo mật ở mức cao nhất, việc hiểu rõ các phương thức tấn công qua Bluetooth và có biện pháp phòng chống là vô cùng quan trọng.

Dưới đây là ba kiểu tấn công Bluetooth phổ biến mà tội phạm mạng có thể sử dụng:

+ *Bluejacking*: Đây là kiểu tấn công gây nhiễu người dùng. Các hacker sử dụng Bluetooth để gửi các tin nhắn Spam cho những người dùng ở trong vùng hoạt động của Bluetooth (khoảng 10m – 20m tùy điều kiện). Bluejacking không thể truy cập vào thông tin của người dùng nhưng nó là tiền đề cho một cuộc tấn công khác (mục tiêu của tin nhắn có thể là quảng cáo hoặc chứa liên kết độc hại để dẫn dụ người dùng nhấp vào). Để phòng chống nó, chỉ đơn giản là người dùng nên để Bluetooth của mình ở chế độ "invisible" hoặc "non-discoverable".

+ *Bluesnarfing*: Không như Bluejacking, Bluesnarfing cho phép hacker lấy thông tin từ thiết bị của nạn nhân. Hacker sử dụng một phần mềm đặt biệt để đánh cắt thông tin thông thông qua giao thức không dây OBEX (Object Exchange) của Bluetooth. Kiểu tấn công này có tác dụng với cả các thiết bị ở chế độ “invisible” nhưng nhược điểm của nó là khá mất thời gian để tìm ra tên thiết bị (invisible mode) thông qua đoán tên thiết bị.

+ *Bluebugging*: Khi người dùng cài đặt Bluetooth ở “discoverable mode”, hacker sử dụng các phương thức của Bluejacking và Bluesnafing để tấn công thiết bị. Hầu hết các thiết bị hiện đại đều miễn nhiễm với loại tấn công này, những thiết bị đã cũ hoặc không nâng cấp firmware là mục tiêu chính của Bluebugging. Hacker gửi các tin nhắn giả mạo nhằm đánh lừa hệ thống nhận diện Buetooth, bình thường thì khi kết nối với thiết bị lạ, máy sẽ hiện 1 mã PIN rồi hỏi xem người dùng có muốn kết nối với thiết bị này hay không nhưng do Bluetooth đã cũ nên sẽ bị hacker kết nối mà không cần thông qua PIN

Tuy Bluetooth có khả năng bị tấn công cao nhưng những phương thức tấn công trên yêu cầu những thiết bị tương đối mắc tiền và đối tượng tấn công ở phạm vi hẹp nên nó không xảy ra nhiều trong thực tế. Cập nhật thiết bị thường xuyên là cách tốt nhất để phòng chống tấn công qua Bluetooth

- Hands-On Hacks

Dù các cuộc tấn công mạng từ xa luôn là mối lo ngại, nhưng tấn công vật lý cũng là một nguy cơ lớn. Nếu hacker có quyền truy cập trực tiếp vào điện thoại, họ có thể thực hiện nhiều hành vi nguy hiểm như:

+ Cài đặt phần mềm gián điệp để theo dõi tin nhắn, cuộc gọi.

+ Tạo "cửa sau" (backdoor) để khai thác Bluetooth, giúp họ truy cập từ xa vào thiết bị sau này (Bluebugging).

+ Sao chép danh bạ, tin nhắn và dữ liệu cá nhân trong thời gian ngắn.

Mặc dù hiện nay, hầu hết điện thoại đều yêu cầu mật mã, vân tay, hoặc nhận diện khuôn mặt để mở khóa, nhưng hacker vẫn có thể khai thác lỗ hổng:

+ Quan sát mã PIN khi người dùng nhập trên màn hình.

+ Sử dụng vân tay khi nạn nhân đang ngủ (đặc biệt là với người quen hoặc người thân xung quanh).

+ Đánh cắp điện thoại vật lý và cố gắng bẻ khóa bằng công cụ chuyên dụng.

- Nguy cơ lừa đảo và ứng dụng độc hại trên điện thoại

Công nghệ ngày càng phát triển, nhưng các phương thức tấn công của hacker cũng không ngừng đổi mới. Một trong những chiến thuật phổ biến nhất là lừa người dùng tự nguyện cung cấp thông tin mà không cần xâm nhập hệ thống. Hai phương thức thường gặp trên thiết bị di động bao gồm:

Phishing – Tấn công lừa đảo trực tuyến

Lừa đảo qua mạng không mới, nhưng trên điện thoại, nó nguy hiểm hơn vì:

+ Thanh địa chỉ ngắn hơn trên trình duyệt di động (Chrome, Firefox Mobile), khiến người dùng khó nhận ra trang web giả mạo.

+ Tốc độ mạng cao giúp trang web tải nhanh chóng, tạo cảm giác tin cậy, khiến người dùng nhập thông tin mà không kịp kiểm tra kỹ.

+ Tấn công qua tin nhắn SMS hoặc ứng dụng OTT (Zalo, Telegram,

WhatsApp) với nội dung dụ dỗ người dùng nhấn vào liên kết độc hại.

Cách phòng chống:

+ Luôn kiểm tra địa chỉ URL trước khi nhập thông tin đăng nhập.

+ Không nhấp vào các liên kết đáng ngờ được gửi qua SMS, email, ứng dụng chat.

+ Bật xác thực hai yếu tố (2FA) để giảm nguy cơ bị chiếm tài khoản ngay cả khi bị lộ mật khẩu.

+ Không lưu mật khẩu trên trình duyệt, thay vào đó hãy sử dụng các trình quản lý mật khẩu uy tín.

Malware Apps – Ứng dụng chứa mã độc

Giống như trên máy tính, các ứng dụng di động có thể chứa mã độc nhằm thu thập dữ liệu người dùng. Dù các chợ ứng dụng như Google Play, App Store đã cải thiện bộ lọc bảo mật, nhưng hacker vẫn có cách vượt qua kiểm duyệt hoặc lợi dụng các kho ứng dụng bên ngoài. Nguy cơ cao hơn đối với người dùng root máy, bẻ khóa hệ điều hành trên thiết bị, hoặc cài đặt ứng dụng từ nguồn không chính thống.

Cách phòng chống:

+ Chỉ tải ứng dụng từ các nguồn chính thống (Play Store, App Store).

+ Không cấp quyền truy cập nhạy cảm (danh bạ, tin nhắn, microphone, camera...) nếu không cần thiết.

+ Hạn chế root/jailbreak điện thoại, vì điều này làm mất cơ chế bảo vệ của hệ điều hành.

+ Sử dụng phần mềm bảo mật và quét virus định kỳ

+ Xóa ngay các ứng dụng không rõ nguồn gốc hoặc ứng dụng yêu cầu quyền truy cập quá mức.

Tấn công kỹ thuật thấp (Low-Tech Hacking)

Không phải mọi cuộc tấn công vào thiết bị di động đều cần đến công nghệ cao hay phần mềm tinh vi. Hacker có thể lợi dụng thói quen sử dụng mật khẩu của người dùng để đánh cắp tài khoản và dữ liệu cá nhân. Dưới đây là hai phương thức tấn công phổ biến:

+ Tận dụng mật khẩu trùng lặp: Người dùng thường có thói quen dùng chung một mật khẩu cho nhiều tài khoản khác nhau như Facebook, Zalo, Gmail,

thậm chí là các diễn đàn cá nhân. Khi một trong các tài khoản này bị lộ (do bị hack hoặc bị lừa đảo qua trang web giả mạo), hacker sẽ thử mật khẩu đó trên các dịch vụ khác. Nếu người dùng sử dụng mật khẩu giống nhau, hacker sẽ dễ dàng truy cập vào nhiều tài khoản quan trọng hơn.

+ Sử dụng mật khẩu mặc định và yếu: Một số dịch vụ hoặc thiết bị khi tạo tài khoản sẽ cấp một mật khẩu mặc định như 123456, 000000, admin, password, nhưng người dùng quên thay đổi. Hacker có thể quét hàng loạt tài khoản để thử các mật khẩu mặc định này và dễ dàng chiếm quyền kiểm soát. Ngoài ra, mật khẩu quá dễ đoán như ngày sinh, số điện thoại, tên cá nhân cũng là một rủi ro lớn.

b. Các nguyên tắc cơ bản khi cài đặt điện thoại thông minh và máy tính bảng trên hệ điều hành Android/iOS

- Lựa chọn thiết bị an toàn

Smartphone là một phần không thể thiếu trong cuộc sống hiện đại, đặc biệt đối với những cá nhân làm việc trong lĩnh vực yêu cầu bảo mật cao như lực lượng công an, luật sư, chính trị gia. Do đó, việc bảo mật thiết bị di động là ưu tiên hàng đầu để ngăn chặn rủi ro bị tấn công mạng và lộ lọt thông tin nhạy cảm.

Iphone được đánh giá là an toàn hơn Android nhờ hệ sinh thái khép kín và cơ chế kiểm soát chặt chẽ của Apple. Apple đảm bảo các bản cập nhật bảo mật liên tục trong ít nhất 5 năm kể từ khi thiết bị được phát hành. Đây là lựa chọn phổ biến của các chính trị gia, luật sư, quan chức chính phủ, những người có nguy cơ cao bị tấn công mạng.

Nếu sử dụng Android, hãy chọn các thiết bị bảo mật tốt. Google Pixel là dòng điện thoại Android có mức bảo mật cao nhất do Google trực tiếp phát triển, thường xuyên được cập nhật bảo mật sớm nhất. Các nhà sản xuất khác như Samsung, OnePlus, Huawei cũng đã cải thiện đáng kể tốc độ phát hành bản vá bảo mật, nhưng vẫn có độ trễ nhất định so với Pixel.

- Cập nhật thường xuyên khi có thể

Người dùng cần luôn cập nhật hệ điều hành và ứng dụng ngay khi có phiên bản mới để bảo vệ thiết bị khỏi các rủi ro bảo mật. Mỗi bản cập nhật của iOS, Android hay các ứng dụng đều vá các lỗ hổng bảo mật mà hacker có thể lợi dụng để xâm nhập vào điện thoại, đánh cắp dữ liệu cá nhân hoặc điều khiển thiết bị từ xa. Nếu không cập nhật kịp thời, thiết bị sẽ trở thành mục tiêu dễ bị tấn công.

Hãy bật chế độ cập nhật tự động để đảm bảo điện thoại luôn chạy phiên

bản mới nhất. Nếu có bản cập nhật lớn, hãy kiểm tra và cài đặt ngay khi có thể, không nên trì hoãn. Đối với ứng dụng, chỉ cập nhật từ App Store hoặc Google Play, tuyệt đối không tải file APK từ nguồn không rõ ràng để tránh nguy cơ nhiễm mã độc.

Hệ điều hành Android còn đặt ra một nguy cơ khác: có rất nhiều ứng dụng trong Google Play Store mà thoạt nhìn có vẻ chính thống, nhưng lại chứa mã độc. Hãy đảm bảo rằng người dùng đã nghiên cứu qua về ứng dụng đó trước khi tải ứng dụng đó về cài đặt. Hãy tìm kiếm với tên của ứng dụng, đọc các bài review, và kiểm tra số lần mà ứng dụng đó đã được cài đặt cho đến hiện tại. Tóm lại: đừng cài đặt một ứng dụng bất kỳ trên điện thoại hay máy tính bảng Android mà không kiểm tra.

Một việc quan trọng nữa là hãy kiểm tra các quyền (permission) được yêu cầu bởi ứng dụng. Một ứng dụng chiếu sáng chẳng hạn không việc gì cần đến việc truy cập danh bạ điện thoại. Người dùng có thể kiểm tra và chỉnh sửa các quyền được cấp cho ứng dụng trên các hệ điều hành iOS và Android mới nhất. Trên Android, hãy vào Settings > Apps, và trên iOS hãy vào Settings > Privacy.

Hình 6. Cửa hàng Google Play

- Kích hoạt mã hóa

Mã hóa đảm bảo rằng dữ liệu trên điện thoại, bao gồm tin nhắn, hình ảnh và các tệp cá nhân, được bảo vệ bằng các khóa bảo mật, ngăn chặn truy cập trái phép. Trên iPhone và hầu hết các thiết bị Android hiện đại, chức năng mã hóa được bật mặc định, nhưng một số dòng máy Android cũ vẫn yêu cầu người dùng kích hoạt thủ công bằng cách vào Settings > Security và bật tùy chọn mã hóa.

Nếu kẻ gian có được điện thoại và kết nối nó vào máy tính, mã hóa sẽ ngăn

họ xem nội dung trừ khi nhập đúng passcode. Passcode chính là chìa khóa giải mã giúp truy cập vào kho dữ liệu số. Vì vậy, người dùng cần đặt mật khẩu mạnh để khóa thiết bị khi không sử dụng, tránh các mã dễ đoán như "123456" hoặc ngày sinh. Nếu có thể, hãy bật xác thực sinh trắc học như vân tay hoặc Face ID để tăng cường bảo mật.

- Sử dụng passcode với ít nhất 6 chữ số và ứng dụng scan vân tay

Bằng cách sử dụng một passcode, người dùng đã ngăn những người khác truy cập vào điện thoại hay máy tính bảng. Hãy chọn một passcode có 6 chữ số mà chỉ có người dùng biết và không sử dụng một passcode đơn giản như 0-0-0-0-0-0, 1-2-3-4-5-6 hay 1-1-2-2-3-3. Người dùng cũng không nên sử dụng ngày tháng năm sinh, tương tự với các tổ hợp thông tin cá nhân khác.

Các điện thoại iPhone và Android cho phép kích hoạt chức năng tự động xóa tất cả các nội dung trên điện thoại nếu như mã đăng nhập sai được gõ vào hơn 10 lần. Chức năng này hoạt động như là một phương pháp bảo mật bổ sung, tuy nhiên nó cũng khá rủi ro nếu như người dùng không có 1 bản backup thiết bị

Trong nhiều trường hợp, việc sử dụng ứng dụng scan vân tay sẽ dễ dàng hơn. Ứng dụng này hoạt động nhanh hơn và an toàn hơn vì một người bất kỳ không thể copy vân tay để mở khóa điện thoại. Nếu người dùng muốn tạm thời tắt đi chức năng scan vân tay, hãy tắt thiết bị iOS (iPhone, iPad,...)/Android và mở/khởi động lại thiết bị. Việc này sẽ bắt người dùng nhập mã passcode vào để đăng nhập thiết bị. Nếu như người dùng không có một ứng dụng scan vân tay trên thiết bị Android, người dùng cũng có thể tạo ra một mẫu pattern để mở khóa điện thoại.

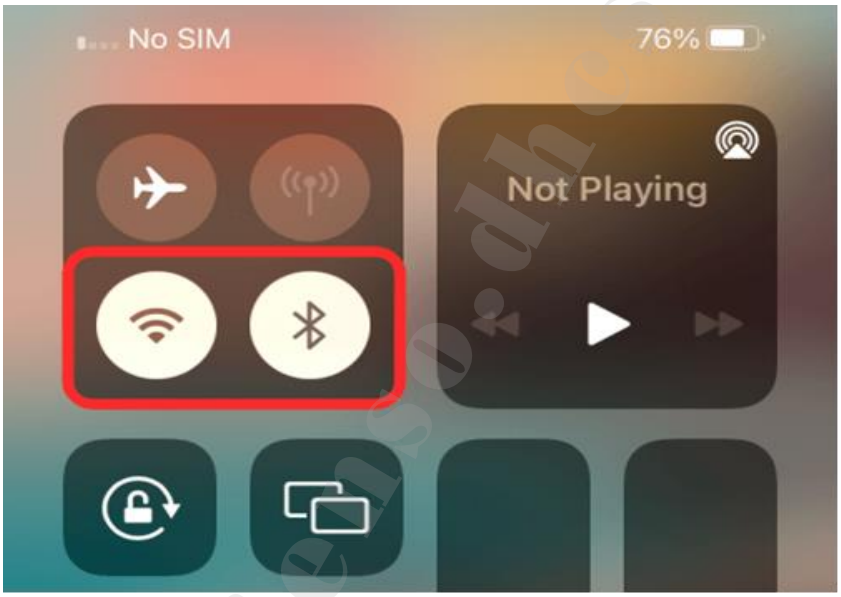
SIM card cũng chứa một passcode. Người dùng có thể sửa passcode này và đổi nó về một mã 6 chữ số khác trong thiết lập cấu hình điện thoại, thay vì sử dụng mã mặc định 0-0-0-0. Một việc nên làm nữa là hãy chuyển toàn bộ danh bạ vào điện thoại và gỡ chúng khỏi SIM card. Nếu như người dùng tình cờ mất điện thoại của mình, thông tin cá nhân các liên lạc không thể được rút trích ra từ SIM card đó.

- Tắt Wifi và Bluetooth khi người dùng không cần dùng đến

Các lực lượng giám sát có thể theo dõi người dùng thông qua WiFi và Bluetooth, ghi nhận lộ trình di chuyển hoặc các địa điểm đã ghé qua, chẳng hạn như theo dõi đường đi đến trạm xe buýt. Để giảm thiểu rủi ro, nếu không cần sử dụng WiFi hay Bluetooth trên đường, hãy tắt chúng bằng cách vào Settings trên thiết bị. Điều này không chỉ bảo vệ quyền riêng tư mà còn giúp tránh khỏi các kỹ thuật tấn công khai thác WiFi và Bluetooth.

Khi người dùng đã từng kết nối với một mạng WiFi, điện thoại sẽ tự động kết nối lại khi ở trong phạm vi phủ sóng. Hacker có thể lợi dụng điều này bằng cách tạo ra các mạng WiFi giả có cùng tên với các mạng phổ biến như Starbucks WiFi hay McDonald's Free WiFi. Nếu thiết bị nhận diện tên mạng đã từng truy cập trước đó, nó sẽ tự động kết nối, khiến dữ liệu cá nhân bị đánh cắp mà không cần sự cho phép của người dùng.

Để bảo vệ bản thân khỏi các cuộc tấn công này, người dùng nên tắt tính năng tự động kết nối WiFi, chỉ kết nối với mạng đáng tin cậy, sử dụng VPN khi truy cập Internet công cộng và không đăng nhập tài khoản quan trọng khi dùng WiFi miễn phí.



Hình 7. Tắt Bluetooth và Wifi trên điện thoại

Một biện pháp bảo mật quan trọng là thường xuyên xóa danh sách các mạng WiFi đã lưu trên thiết bị di động để tránh nguy cơ bị tấn công qua mạng giả mạo. Nếu đã kết nối với mạng WiFi ở khách sạn, quán cà phê hay nơi công cộng, hãy gỡ mạng đó khỏi bộ nhớ thiết bị ngay sau khi sử dụng. Điều này giúp ngăn chặn thiết bị tự động kết nối vào các mạng giả mạo có cùng tên, do hacker tạo ra để đánh cắp dữ liệu cá nhân.

Để thực hiện, người dùng có thể vào phần cài đặt (Settings) trên thiết bị, truy cập danh sách các mạng WiFi đã kết nối, chọn mạng cần xóa và nhấn "Forget this network" (Quên mạng này). Ngoài ra, nên tắt tính năng tự động kết nối với WiFi trên cả Android và iOS để đảm bảo thiết bị chỉ kết nối khi có sự cho phép của người dùng, giúp giảm thiểu nguy cơ bị tấn công mạng.

- Tắt chức năng cho phép xem trước thông báo trên màn hình điện thoại

được khóa

Tắt chức năng xem trước thông báo trên màn hình khóa là một biện pháp bảo mật quan trọng để bảo vệ thông tin nhạy cảm khỏi những người xung quanh hoặc kẻ xấu có thể nhìn trộm. Các thông báo có thể chứa mật khẩu tạm thời, mã xác thực đăng nhập (OTP), hay tin nhắn riêng tư từ WhatsApp, Zalo hoặc SMS. Nếu thông báo hiển thị trên màn hình khóa, bất kỳ ai cầm điện thoại cũng có thể đọc được mà không cần mở khóa thiết bị.

Để bảo vệ thông tin, hãy ẩn nội dung thông báo trên màn hình khóa:

Trên iOS (iPhone):

+ Vào Cài đặt (Settings) > Thông báo (Notifications)

+ Chọn Hiển thị bản xem trước (Show Previews)

+ Chọn "Khi được mở khóa" (When Unlocked)

Trên Android:

+ Vào Cài đặt (Settings) > Ứng dụng & Thông báo (Apps & Notifications)

+ Chọn Thông báo trên màn hình khóa (Lock Screen Notifications)

+ Chọn "Ẩn nội dung nhạy cảm" hoặc "Không hiển thị thông báo"

Sau khi bật tùy chọn này, thông báo sẽ vẫn xuất hiện trên màn hình khóa, nhưng nội dung bên trong sẽ chỉ hiển thị sau khi thiết bị được mở khóa, giúp đảm bảo không ai có thể đọc thông tin quan trọng khi chưa có quyền truy cập.

4. Các nguyên tắc khi sử dụng mạng xã hội

a. Các nguyên tắc khi sử dụng mạng xã hội để đảm bảo an ninh, an toàn thông tin

Mạng xã hội là nơi chúng ta chia sẻ rất nhiều thông tin cá nhân, nhưng đôi khi việc chia sẻ quá mức lại vô tình tạo cơ hội cho hacker và kẻ xấu khai thác. Một trong những phương pháp thu thập dữ liệu phổ biến mà tin tặc sử dụng là **Open Source Intelligence (OSINT)** – kỹ thuật thu thập thông tin từ nguồn mở để phục vụ các cuộc tấn công mạng hoặc lừa đảo danh tính.

- Cẩn trọng với thông tin cá nhân khi đăng tải

Người dùng thường có thói quen đăng tải hình ảnh hộ chiếu, bằng lái xe, vé máy bay, vé xem ca nhạc, mà không nhận ra rằng mã vạch (barcode) trên vé có thể bị sử dụng để truy cập vào tài khoản hoặc đánh cắp danh tính. Chỉ cần một bức ảnh rõ ràng, kẻ gian có thể tạo tài khoản giả mạo, vay tiền dưới tên chúng ta,

hoặc thậm chí đánh cắp thông tin cá nhân quan trọng.

Hạn chế chia sẻ thông tin về lịch trình cá nhân. Việc đăng tải địa điểm đang ở, kế hoạch đi du lịch, nơi làm việc, số điện thoại có thể giúp kẻ xấu theo dõi thói quen, xác định thời điểm bạn không có mặt tại nhà để thực hiện hành vi trộm cắp hoặc tiếp cận bạn với mục đích xấu.

- Kiểm soát quyền riêng tư trên mạng xã hội.

Nhiều công ty chỉ yêu cầu tên, ngày tháng năm sinh và địa chỉ để xác thực người dùng là người mà người dùng cho họ biết. Thông tin này gần như có thể dễ dàng tìm kiếm online. Mọi người thường chúc mừng sinh nhật lẫn nhau trên các mạng truyền thông và vô tình cho biết họ sống ở đâu, chỉ bởi đã chia sẻ một bức hình ngôi nhà mới của họ lên Instagram. Sử dụng phương pháp này, một hacker nếu lừa/thỏa hiệp được với nhân viên một nhà mạng để đăng ký số điện thoại người khác với tên của người đó. Việc này cho phép kẻ xấu đó truy cập được các tin nhắn mới trên WhatsApp. Phương pháp hacking này còn được biết với tên gọi social engineering; đây là một dạng tấn công mạng có tương tác và điều khiển hành vi con người. Những câu trả lời cho các câu hỏi bí mật cũng có thể thường được tìm kiếm online. Nó có thể là tên gọi của con thú cưng đầu tiên, hay ngày sinh nhật của mẹ người dùng. Hãy chú ý điều này. Sẽ luôn tốt hơn nếu người dùng sinh ra các password ngẫu nhiên để trả lời cho các câu hỏi bí mật này. Người dùng có thể lưu các password là câu trả lời cho các câu hỏi bí mật này trong một ứng dụng quản lý password (password manager).

b. Các nguyên tắc cơ bản kiểm tra bảo mật cho tài khoản

- Thử tìm kiếm với Google thông tin riêng tư, cá nhân

Khi hacker muốn thu thập thông tin về một cá nhân để thực hiện tấn công, bước đầu tiên thường là tìm kiếm tên của đối tượng trên Google. Đây là cách đơn giản nhưng hiệu quả để tìm ra tài khoản mạng xã hội, bài đăng cũ, thông tin liên lạc, địa chỉ nhà, nơi làm việc hoặc thậm chí dữ liệu nhạy cảm.

Để kiểm soát và bảo vệ thông tin cá nhân trên Internet, người dùng nên thường xuyên tìm kiếm tên mình trên Google bao gồm cả biệt danh, số điện thoại, email… để xem những dữ liệu nào đang hiển thị công khai. Nếu phát hiện thông tin nhạy cảm bị lộ, có thể yêu cầu gỡ bỏ thông tin khỏi công cụ tìm kiếm.

Người dùng nên thiết lập thông báo với Google để được email mỗi khi tên xuất hiện kết quả mới với Google. Trong một số trường hợp, thậm chí người dùng có thể gỡ bỏ thông tin này khỏi công cụ tìm kiếm này.

- Thiết lập riêng tư cho các bài viết và log out tài khoản

Chúng ta chia sẻ rất nhiều thông tin cá nhân trên các nền tảng mạng xã hội, và điều này có thể tạo ra rủi ro về bảo mật. Vì vậy, việc thiết lập quyền riêng tư cho tài khoản là rất quan trọng. Nếu người dùng thường xuyên chia sẻ cuộc sống cá nhân trên Facebook hoặc Instagram, hãy đảm bảo tài khoản Facebook được đặt ở chế độ riêng tư bằng cách vào Cài đặt quyền riêng tư và giới hạn ai có thể xem bài đăng. Đồng thời, hãy chuyển tài khoản Instagram sang chế độ riêng tư để chỉ những người được phê duyệt mới có thể theo dõi và xem nội dung của người dùng. Nếu sử dụng Snapchat, hãy kiểm tra cài đặt để đảm bảo chỉ bạn bè mới có thể gửi tin nhắn hoặc xem câu chuyện của mình.

Với X (trước đây là Twitter), nền tảng này thường được sử dụng để tiếp cận số lượng lớn người theo dõi, nhưng điều đó cũng có nghĩa là thông tin cá nhân có thể dễ dàng bị lộ ra ngoài. Nếu không muốn tài khoản X công khai, hãy vào Cài đặt bảo mật, bật chế độ bảo vệ bài đăng để chỉ những người theo dõi mới có thể xem nội dung của người dùng. Đặc biệt, tắt chia sẻ vị trí trong bài đăng để tránh lộ thông tin di chuyển cá nhân. Ngoài ra, nếu đăng nhập vào tài khoản X trên máy tính công cộng hoặc thiết bị của người khác, hãy luôn đăng xuất sau khi sử dụng để tránh bị người khác truy cập trái phép.

- Tạo các bản copy điện tử an toàn cho định danh (ID)

Người dùng có thể tạo bản sao điện tử an toàn cho các giấy tờ định danh như CCCD gắn chip, hộ chiếu, giấy phép lái xe hoặc các loại giấy tờ tùy thân khác để sử dụng khi cần mà không lo bị lộ thông tin cá nhân nhạy cảm. Tại Việt Nam, ứng dụng VNeID do Bộ Công an phát triển giúp người dân quản lý thông tin định danh điện tử một cách an toàn và tiện lợi.

Ứng dụng VNeID cho phép người dùng lưu trữ và xuất trình các giấy tờ quan trọng dưới dạng điện tử, giúp giảm rủi ro khi mang theo giấy tờ gốc. Người dùng có thể sử dụng VNeID để xác minh danh tính, thực hiện các thủ tục hành chính, khai báo y tế, đăng ký thường trú/tạm trú trực tuyến mà không cần xuất trình bản giấy. Ngoài ra, VNeID giúp bảo vệ thông tin cá nhân nhờ tích hợp tính năng bảo mật cao, hạn chế nguy cơ bị giả mạo hoặc đánh cắp dữ liệu.

Để đảm bảo an toàn, người dùng nên cập nhật thông tin chính xác trên VNeID, chỉ xuất trình khi cần thiết và không chia sẻ ảnh chụp mã QR hoặc thông tin trên ứng dụng với người lạ. Nếu cần cung cấp bản sao giấy tờ, hãy sử dụng tính năng tạo bản sao có xác thực trên ứng dụng để đảm bảo tính hợp lệ và bảo mật.

- Kiểm tra các thiết bị đã được đăng nhập

Người dùng cần chủ động kiểm soát các thiết bị đã đăng nhập vào tài khoản cá nhân để đảm bảo an toàn thông tin. Nếu đã từng đăng nhập vào tài khoản trên máy tính công cộng, máy tính bảng của người khác hoặc thiết bị không thuộc quyền sở hữu, hãy chắc chắn rằng mình đã đăng xuất (log out) hoàn toàn khi không còn sử dụng.

Để kiểm tra và quản lý các phiên đăng nhập còn hoạt động (active sessions), người dùng có thể truy cập vào cài đặt bảo mật của các dịch vụ như Google, Facebook, Zalo, WhatsApp… Những nền tảng này đều cung cấp danh sách thiết bị đang đăng nhập vào tài khoản, bao gồm loại thiết bị, vị trí, thời gian hoạt động gần nhất. Nếu phát hiện thiết bị lạ hoặc phiên đăng nhập đáng ngờ, người dùng cần ngay lập tức đăng xuất (log out) từ xa và đổi mật khẩu để bảo vệ tài khoản.

Ngoài ra, người dùng nên bật xác thực hai yếu tố (2FA) để tăng cường bảo mật. Mỗi lần đăng nhập từ một thiết bị mới, hệ thống sẽ yêu cầu nhập mã xác nhận được gửi về số điện thoại hoặc email, giúp ngăn chặn truy cập trái phép.

- Thực hiện kiểm tra bảo mật định kỳ

Người dùng nên thực hiện kiểm tra bảo mật định kỳ để đảm bảo tài khoản và thông tin cá nhân luôn được bảo vệ. Nhiều nền tảng lớn như Google, Facebook, X (Twitter), Zalo đều cung cấp công cụ giúp kiểm tra các thiết lập bảo mật, danh sách các thiết bị đang đăng nhập, cũng như các ứng dụng/dịch vụ bên thứ ba có quyền truy cập vào tài khoản.

Việc kiểm tra định kỳ giúp người dùng dễ dàng phát hiện thiết bị lạ, phiên đăng nhập không nhận biết được hoặc ứng dụng không còn sử dụng nhưng vẫn có quyền truy cập dữ liệu cá nhân. Nếu phát hiện bất kỳ hoạt động đáng ngờ nào, người dùng nên thu hồi quyền truy cập của ứng dụng đó, đăng xuất khỏi thiết bị lạ và đổi mật khẩu nếu cần thiết.

Ngoài ra, người dùng cũng nên bật tính năng cảnh báo bảo mật (Security Alerts), để nhận được thông báo mỗi khi có hoạt động đăng nhập bất thường. Thực hiện kiểm tra bảo mật định kỳ không chỉ giúp bảo vệ tài khoản cá nhân mà còn hạn chế rủi ro bị tấn công mạng.

II. KỸ NĂNG PHÒNG, CHỐNG LỘ, MẤT BÍ MẬT NHÀ NƯỚC TRÊN KHÔNG GIAN MẠNG

1. Mục tiêu, yêu cầu.

- Đảm bảo an toàn tuyệt đối cho BMNN trong mọi tình huống; chủ động

phát hiện, xóa bỏ những nguyên nhân, điều kiện làm lộ, mất bí mật nhà nước trên không gian mạng và những sơ hở, thiếu sót mà các thế lực thù địch, các loại tội phạm và phần tử xấu có thể lợi dụng để thu thập, chiếm đoạt BMNN.

- Chủ động phòng ngừa, phát hiện, đấu tranh làm thất bại âm mưu, hoạt động thu thập bí mật nhà nước của các loại đối tượng.

- Điều tra, xử lý kịp thời, nghiêm minh những hành vi làm lộ, mất bí mật nhà nước trên không gian mạng.

- Tăng cường năng lực bảo vệ bí mật nhà nước của các cơ quan, tổ chức, đảm bảo việc xử lý thông tin an toàn, hạn chế tối đa rủi ro bị đánh cắp hoặc lợi dụng.

2. Tổ chức phòng, chống lộ, mất bí mật nhà nước trên không gian mạng.

Phòng, chống lộ BMNN trên không gian mạng nhằm đảm bảo an toàn tuyệt đối cho BMNN trong mọi tình huống; chủ động phát hiện, xóa bỏ những nguyên nhân, điều kiện làm lộ, mất BMNN trên không gian mạng và những sơ hở, thiếu sót mà các thế lực thù địch, các loại tội phạm và phần tử xấu có thể lợi dụng để thu thập, chiếm đoạt BMNN. Qua đó, chủ động phòng ngừa, phát hiện, đấu tranh làm thất bại âm mưu, hoạt động thu thập BMNN của các loại đối tượng; điều tra, xử lý kịp thời những hành vi làm lộ, mất BMNN trên không gian mạng và nâng cao khả năng phòng ngừa, bảo vệ BMNN của các cơ quan, tổ chức và cá nhân.

Để phòng, chống lộ lọt, mất BMNN trên không gian mạng, cán bộ công an cần có một số kỹ năng sau:

a. Nắm tình hình, phát hiện lộ BMNN trên không gian mạng:

- Cán bộ công an cần nắm tình hình về: phương thức, thủ đoạn lợi dụng hệ thống thiết bị, phương tiện, dịch vụ Internet, công nghệ thông tin để thu thập BMNN, bí mật nội bộ của các đối tượng thù địch, CQĐB nước ngoài; dấu hiệu "tự diễn biến", "tự suy thoái" trong nội bộ; các vụ lộ bí mật nhà nước trên không gian mạng, những sơ hở, thiếu sót trong bảo vệ bí mật nhà nước của các cơ quan, đơn vị, nhất là trong việc lưu trữ, sử dụng, bảo quản bí mật nhà nước trên hệ thống thông tin,... Công tác nắm tình hình hoạt động lộ BMNN trên không gian mạng được tiến hành lồng ghép, đan xen với nắm tình hình chung, nắm tình hình toàn diện về đối tượng, địa bàn, lĩnh vực.

- Biện pháp để nắm tình hình, phát hiện lộ BMNN đó là:

+ Trong công tác, cán bộ công an chú ý theo dõi, kiểm soát an ninh thông

tin trên mạng Internet: tập trung theo dõi các tờ báo, website của các cơ quan thông tấn, báo chí, truyền thông; theo dõi các Website, blog, diễn đàn, hộp thư điện tử, trang mạng xã hội của các đối tượng phản động, tổ chức chống đối trong và ngoài nước.

+ Cán bộ công an tại các đơn vị nghiệp vụ về an ninh mạng cần sử dụng biện pháp kỹ thuật nghiệp vụ để trinh sát, kiểm soát, phát hiện các vụ lộ BMNN trên không gian mạng.

+ Đề xuất thanh tra, kiểm tra phát hiện lộ BMNN trên không gian mạng đối với các cơ quan, tổ chức, đơn vị trực tiếp chứa đựng thông tin BMNN.

b. Tuyên truyền, vận động quần chúng tham gia bảo vệ BMNN trên không gian mạng

- Về đối tượng cần tập trung công tác tuyên truyền:

Trước hết và chủ yếu là những người nắm giữ BMNN; những người làm công tác soạn thảo, lưu giữ, chuyển giao, sử dụng BMNN; những người làm công tác bảo vệ BMNN (cả chuyên trách và kiêm nhiệm) ở các cơ quan, đơn vị, doanh nghiệp; cán bộ làm nhiệm vụ quản trị, biên tập bài viết trên trang, cổng thông tin điện tử của cơ quan, đơn vị.

- Nội dung tuyên truyền, cần tập trung vào những vấn đề chủ yếu như:

+ Tuyên truyền phổ biến danh mục BMNN được quy định trong pháp luật bảo vệ BMNN;

+ Vị trí, vai trò, tầm quan trọng của việc bảo vệ BMNN, những hậu quả thiệt hại nghiêm trọng đối với an ninh quốc gia, lợi ích quốc gia, dân tộc khi để lộ, mất BMNN;

+ Nguyên nhân dẫn đến lộ BMNN trên không gian mạng, trong đó cần đi sâu làm rõ những nguyên nhân chủ quan dẫn đến lộ BMNN, âm mưu, phương thức, thủ đoạn thu thập BMNN qua mạng Intnernet của các thế lực thù địch, tội phạm, các hình thức lộ BMNN trên không gian mạng;

+ Quy định của pháp luật về bảo vệ BMNN, trong đó tập trung chỉ rõ trách nhiệm bảo vệ BMNN và cách thức tiến hành công tác bảo vệ BMNN trên không gian mạng.

- Về phương pháp tiến hành:

+ Lực lượng An ninh mạng cần chủ động phối hợp với các cơ quan Tuyên giáo, Thông tin truyền thông, các cơ quan, ban, ngành ở Trung ương và địa

phương làm tốt công tác tuyên truyền, phổ biến, giáo dục pháp luật về bảo vệ BMNN cho cán bộ, đảng viên, công chức, viên chức, nhất là cán bộ công tác tại bộ phận thiết yếu, cơ mật, chứa đựng BMNN; cán bộ trực tiếp soạn thảo, chuyển nhận, lưu trữ, bảo quản BMNN hoặt thường xuyên tiếp xúc BMNN.

+ Phối hợp với các cơ quan, đơn vị tổ chức các lớp tập huấn, bồi dưỡng nâng cao kiến thức về bảo vệ BMNN, cập nhật những tiến bộ khoa học kỹ thuật và công nghệ thông tin cho lãnh đạo và cán bộ trực tiếp làm công tác bảo vệ BMNN.

+ Coi trọng bồi dưỡng, lồng ghép nội dung công tác bảo vệ BMNN thông qua các lớp tập huấn nâng cao kiến thức, kỹ năng về công nghệ viễn thông, tin học, Internet cho cán bộ, đảng viên, công nhân viên trong các cơ quan, tổ chức.

c. Ứng dụng các giải pháp về khoa học, công nghệ phòng chống lộ BMNN trên không gian mạng

- Nghiên cứu, xây dựng, phát triển các phần mềm diệt virus, nâng cao hiệu quả hoạt động của "tường lửa" (Firewall) nhằm ngăn chặn các cuộc tấn công mạng, phát tán virus gián điệp xâm nhập lấy cắp, chiếm đoạt BMNN.

- Sử dụng các công cụ bảo vệ hệ thống cơ sở dữ liệu, đảm bảo cho các cổng dịch vụ Internet (ICP), các trung tâm dữ liệu kết nối Internet; triển khai ứng dụng các biện pháp kỹ thuật tác chiến tin học nghiệp vụ, công cụ đảm bảo an ninh và an toàn cho hệ thống thiết bị tin học, cơ sở dữ liệu và các phần mềm nghiệp vụ.

- Phối hợp với các đơn vị nghiệp vụ có liên quan sử dụng các phương tiện kỹ thuật chuyên dùng để giám sát từ xa, phát hiện, cảnh báo, ngăn chặn vi phạm nguyên tắc trong thông tin, liên lạc có thể dẫn đến lộ, mất bí mật, phát hiện các vụ lộ, mất bí mật nhà nước qua hệ thống thông tin, kiểm soát thông tin với các địa chỉ liên lạc nghi vấn có hoạt động thu thập bí mật nhà nước.

- Sử dụng các phần mềm, công cụ, hệ thống chuyên dụng tổ chức trinh sát máy tính, thiết bị di động và giám sát hoạt động trên mạng viễn thông, Internet của các đối tượng liên quan an ninh quốc gia, thu thập thông tin, tài liệu nhằm phát hiện, đấu tranh ngăn chặn hoạt động lợi dụng hệ thống thông tin thu thập bí mật nhà nước.

- Phối hợp với Bộ Thông tin và Truyền thông (hiện tại là Bộ Khoa học và Công nghệ) cũng như các doanh nghiệp cung cấp dịch vụ viễn thông, Internet nhằm ngăn chặn truy nhập từ trong nước đối với các trang mạng blog đăng tải nội dung bí mật nhà nước, góp phần hạn chế việc phát tán tài liệu bí mật nhà nước

cũng như lợi dụng bí mật nhà nước đã thu thập được gây phương hại đến an ninh quốc gia.

d. Tham mưu cho Đảng, Nhà nước và phối hợp với các cơ quan, đơn vị tổ chức phòng, chống lộ, mất bí mật nhà nước trên không gian mạng

- Tham mưu cho Đảng, Nhà nước, Quốc hội hoàn thiện hệ thống pháp luật về bảo vệ BMNN nói chung, hệ thống các quy phạm điều chỉnh tổ chức, cá nhân trong sử dụng mạng Internet liên quan đến công tác bảo vệ BMNN.

- Tham mưu, hướng dẫn các cơ quan, tổ chức, địa phương chấp hành các quy định của pháp luật về bảo vệ BMNN, không để lộ BMNN trên không gian mạng. Qua công tác nghiệp vụ, bảo vệ an ninh chính trị nội bộ, công tác kiểm tra, thanh tra, kịp thời phát hiện những sơ hở, thiếu sót để kiến nghị các cơ quan, tổ chức, địa phương có biện pháp chấn chỉnh, khắc phục kịp thời; nêu cảnh báo về các nguy cơ lộ, mất BMNN trên không gian mạng để các cơ quan, tổ chức, địa phương nâng cao tinh thần cảnh giác, chủ động phòng ngừa;

- Thường xuyên phối hợp, hướng dẫn các cơ quan, đơn vị có biện pháo khắc phục các "lỗ hổng" bảo mật; ngăn chặn các cuộc tấn công mạng, chiến dịch gián điệp mạng của tin tặc nước ngoài; rà soát các thiết bị không rõ nguồn gốc, xuất xứ hoặc có nguồn gốc từ các Tập đoàn, Công ty của Trung Quốc, Đài Loan và các nước khác được cảnh báo nguy cơ cao mất an toàn thông tin (Huawei, ZTE) để đề xuất cơ quan chức năng tổ chức kiểm định đảm bảo về an ninh, an toàn thông tin trước khi đưa vào sử dụng.

- Phối hợp, hướng dẫn các cơ quan, đơn vị xây dựng và thực hiện nghiêm chế độ, nội qui, qui chế; phương án, kế hoạch bảo vệ bí mật nhà nước ở các cơ quan, tổ chức.

- Hướng dẫn các cơ quan, đơn vị trong tuyên truyền phổ biến pháp luật về an ninh thông tin nói chung, pháp luật về bảo vệ bí mật nhà nước nói riêng, nâng cao tinh thần cảnh giác, ý thức trách nhiệm bảo vệ bí mật nhà nước cho cán bộ, nhân viên trong cơ quan, tổ chức, doanh nghiệp.

e. Tổ chức điều tra, xử lý các đối tượng, hành vi làm lộ, mất hoặc xâm hại đến bí mật nhà nước

- Yêu cầu:

+ Ngăn chặn không để bí mật nhà nước tiếp tục bị lộ và khắc phục, hạn chế hậu quả, thiệt hại xảy ra;

+ Làm rõ tổ chức, cá nhân vi phạm và tính chất, mức độ vi phạm để tính

toán biện pháp xử lý và chấn chỉnh công tác bảo vệ bí mật nhà nước;

+ Đảm bảo bí mật các biện pháp, công tác nghiệp vụ, đặc biệt là biện pháp kỹ thuật nghiệp vụ.

- Tổ chức điều tra, xử lý:

+ Thu thập, nghiên cứu, phân tích bí mật nhà nước thu được bị lộ trên không gian mạng

+ Nội dung cần thu thập: Thông tin về bí mật nhà nước đã bị lộ: mức độ mật của tài liệu; cơ quan, đơn vị ban hành văn bản; cơ quan, đơn vị và cá nhân có trách nhiệm quản lý, sử dụng văn bản (nếu có phản ánh); chữ ký của người ký duyệt văn bản; các bút phê, ý kiến chỉ đạo của lãnh đạo các cấp phản ánh trên văn bản; các dấu vết khác trên văn bản có kèm theo… Thông tin ban đầu về cá nhân, tổ chức đăng tải tài liệu bí mật, website đăng tải, thời gian đăng tải.

+ Xác định bí mật nhà nước bị lộ thuộc lĩnh vực nào? Của ngành nào, cơ quan, tổ chức nào ban hành;… Trên cơ sở đó, gửi công văn yêu cầu cơ quan có liên quan, thành lập Hội đồng thẩm định mức độ mật của tài liệu làm căn cứ để triển khai các biện pháp tiếp theo.

- Triển khai các biện pháp nhằm xác định cá nhân làm lộ bí mật nhà nước và những người có liên quan:

+ Phối hợp với các lực lượng ngăn chặn bí mật nhà nước tiếp tục bị lộ và khắc phục hậu quả, thiệt hại có thể xảy ra. Do đặc điểm dễ lan truyền, bí mật nhà nước bị lộ trên internet thường được các cá nhân, tổ chức sao chép và chia sẻ trên nhiều trang mạng khác nhau gây hậu quả

+ Phối hợp với cơ quan, tổ chức và cá nhân có liên quan dựng lại đường đi của tài liệu, trên cơ sở đó, xác định cá nhân làm lộ và những người có liên quan.

+ Triển khai trưng cầu giám định kỹ thuật hình sự đối với tài liệu bí mật nhà nước bị lộ.

+ Triển khai các biện pháp nghiệp vụ xác minh, làm rõ các cá nhân, tổ chức vi phạm.

- Áp dụng biện pháp xử lý đối với tổ chức, cá nhân vi phạm: Dựa trên việc triển khai các biện pháp bảo vệ bí mật nhà nước, lực lượng An ninh tiến hành điều tra, phân tích và đưa ra kết luận về nguyên nhân, phương thức và đối tượng đã thực hiện hành vi thu thập, phát tán thông tin mật trên internet. Đồng thời, lực lượng An ninh xác định những cá nhân, tổ chức có liên quan để đề xuất biện pháp xử lý phù hợp, bao gồm việc khắc phục hậu quả của thông tin bị lộ, thu hồi hoặc

hạn chế truy cập, cũng như xử lý trách nhiệm theo quy định pháp luật đối với các cá nhân, tổ chức vi phạm.

- Kiến nghị cơ quan, tổ chức có trách nhiệm quản lý, sử dụng bí mật nhà nước tăng cường công tác bảo vệ bí mật nhà nước: Thường xuyên tổ chức tuyên truyền, phổ biến các quy định pháp luật về bảo vệ bí mật nhà nước nhằm nâng cao nhận thức và trách nhiệm của cán bộ, công chức, viên chức và nhân dân. Đồng thời, tăng cường công tác kiểm tra, giám sát việc tuân thủ các quy định pháp luật về bảo vệ bí mật nhà nước cũng như các quy định về quản lý, sử dụng Internet trong các cơ quan, tổ chức. Bên cạnh đó, cần bổ sung, hoàn thiện các quy chế, quy định nội bộ về bảo vệ bí mật nhà nước để phù hợp với tình hình thực tế. Ngoài ra, cần đầu tư, nâng cấp các phương tiện, thiết bị kỹ thuật hiện đại phục vụ công tác bảo mật, đồng thời kiện toàn đội ngũ cán bộ chuyên trách, đảm bảo đủ năng lực và trình độ để thực hiện hiệu quả nhiệm vụ bảo vệ bí mật nhà nước.

DANH MỤC TÀI LIỆU THAM KHẢO

1. An toàn, an ninh mạng: *Thực trạng và khuyến cáo*, https://vjst.vn/vn/tin-tuc/8126/an-toan--an-ninh-mang-thuc-trang-va-khuyen-cao.aspx, truy cập ngày 05/3/2025.

2. Trần Bình (2023), *Tấn công mạng sẽ vẫn diễn biến phức tạp trong 2024*, https://www.sggp.org.vn/tan-cong-mang-se-van-dien-bien-phuc-tap-trong-2024-post718026.html, truy cập ngày 31/12/2023.

3. Bộ Công an (2021), *Đảm bảo chủ quyền quốc gia trên không gian mạng, Kỷ yếu hội thảo khoa học cấp quốc gia,* Nxb Quốc gia Sự thật, Tập 1-2, Hà Nội.

4. Công ty Cổ phần Công nghệ An ninh mạng Quốc gia Việt Nam (NCS), *Tổng kết An ninh mạng Việt Nam năm 2023 và dự báo 2024*, https://ncsgroup.vn/tong-ket-an-ninh-mang-viet-nam-nam-2023-va-du-bao-2024/, truy cập ngày 31/12/2023.

5. Trần Văn Hòa, Nguyễn Ngọc Cương (2019), *Phòng, chống tội phạm trên không gian mạng*, Nxb CAND, Hà Nội.

6. Cục A05, *Báo cáo tổng kết công tác năm 2023 và phương hướng nhiệm vụ công tác năm 2024,* Hà Nội 2024.

7. Văn phòng Bộ Công an (V01), *Báo cáo sơ kết công tác 6 tháng đầu năm 2024,* Hà Nội 2024

8. Tô Lâm (2021), *Chủ quyền Không gian mạng. Yêu cầu thời đại và nghĩa vụ quốc gia.* NXB CAND, Hà Nội.

9. Bùi Anh Hiếu (2021), *Điều tra và phân tích bằng chứng bằng cách sử dụng FTK Images,* Báo cáo phòng chống và điều tra tội phạm máy tính, Học viện Kỹ thuật mật mã, Hà Nội.

10. Quốc hội nước Cộng hòa XHCN Việt Nam, *Luật Bảo vệ BMNN, số 29/2018/QH14,* Hà Nội (2018).

11. Quốc hội nước Cộng hòa XHCN Việt Nam, *Luật An ninh mạng, số 24/2018/QH14,* Hà Nội (2018).

12. Chính phủ nước Cộng hòa XHCN Việt Nam , *Nghị định 13/2023/NĐ-CP về Bảo vệ dữ liệu cá nhân,* Hà Nội (2023).

MỤC LỤC