BAN QUẢN LÝ
KHU CÔNG NGHỆ CAO
VÀ CÁC KHU CÔNG NGHIỆP ĐÀ NẴNG

CÔNG AN THÀNH PHỐ ĐÀ NẴNG
PHÒNG AN NINH MẠNG VÀ PCTP
SỬ DỤNG CÔNG NGHỆ CAO

TẬP HUẤN

MỘT SỐ NỘI DUNG BẢO ĐẢM AN NINH MẠNG, BẢO VỆ BÍ MẬT NHÀ NƯỚC TRÊN KHÔNG GIAN MẠNG, BẢO VỆ DỮ LIỆU CÁ NHÂN

Thượng tá, Ths. **LÊ CAO TÂM**
Trưởng Phòng An ninh mạng
và PCTP sử dụng công nghệ cao

CHỦ TRƯƠNG, CHÍNH SÁCH, PHÁP LUẬT VỀ AN NINH MẠNG

Luật An ninh mạng 2018

Nghị quyết số 30-NQ/TW ngày 25/7/2018 của Bộ Chính trị về Chiến lược An ninh mạng quốc gia.

Quyết định số 964/QĐ-TTg ngày 10/8/2022 của Thủ tướng Chính phủ Phê duyệt Chiến lược An toàn, an ninh mạng quốc gia, chủ động ứng phó với các thách thức từ không gian mạng đến năm 2025, tầm nhìn đến năm 2030.

Quyết định số 77/QĐ-TTg ngày 30/11/2022 của Thủ tướng Chính phủ Phê duyệt Đề án "Xây dựng Thế trận An ninh nhân dân trên không gian mạng"

Nghị định số 53/2022/NĐ-CP ngày 15/8/2022 của Chính phủ quy định chi tiết một số điều của Luật An ninh mạng.

Nghị định số 13/2023/NĐ-CP ngày 17/4/2023 của Chính phủ về Bảo vệ dữ liệu cá nhân.

CHỦ TRƯƠNG, CHÍNH SÁCH, PHÁP LUẬT VỀ AN NINH MẠNG

- Nghị định số 144/2021/NĐ-CP ngày 31/12/2021 của Chính phủ.
- Nghị định số 14/2022/NĐ-CP ngày 27/01/2022 của Chính phủ.
- Hiện Bộ Công an đã trình Dự thảo Nghị định của Chính phủ quy định xử phạt vi phạm hành chính trong lĩnh vực an ninh mạng.

"**An ninh mạng** là sự bảo đảm hoạt động trên không gian mạng không gây phương hại đến an ninh quốc gia, trật tự, an toàn xã hội, quyền và lợi ích hợp pháp của cơ quan, tổ chức, cá nhân."

Theo khoản 1 Điều 2 Luật An ninh mạng 2018

AN NINH MẠNG

An ninh thông tin

- Bảo vệ BMNN trên không gian mạng.
- Phản bác thông tin xấu độc, xử lý tin giả.

An toàn thông tin

- Một số hình thức tấn công mạng.
- Biện pháp an toàn trên không gian mạng.

PCTP sử dụng cnc

- Các phương thức, thủ đoạn lừa đảo.
- Bảo vệ dữ liệu cá nhân.

BẢO VỆ
BÍ MẬT NHÀ NƯỚC
trên không gian mạng

350 vụ

làm lộ, mất bí mật nhà nước trên không gian mạng
theo thống kê của Bộ Công an trong giai đoạn từ 2015-2021

TÌNH HÌNH LỘ, MẤT BMNN TRÊN KHÔNG GIAN MẠNG

- **57,7%** là bí mật nhà nước bị lộ qua việc đăng tải công khai thông tin trên các website và cổng thông tin, trang điện tử của các cơ quan nhà nước, ban, ngành.
- **1,6%** là việc sử dụng dịch vụ thư điện tử như Gmail, Yahoo Mail để gửi, nhận tài liệu có chứa nội dung bí mật nhà nước.
- **9,3%** là lộ bí mật nhà nước qua các trang mạng xã hội.

QUY ĐỊNH CỦA PHÁP LUẬT VỀ BẢO VỆ BMNN TRÊN KHÔNG GIAN MẠNG

Điều 5 Luật Bảo vệ bí mật nhà nước quy định các hành vi bị nghiêm cấm liên quan đến không gian mạng như sau:

- Soạn thảo, lưu giữ tài liệu có chứa nội dung bí mật nhà nước 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 giữu bí mật nhà nước theo quy định của pháp luật về cơ yếu.
- Truyền đưa bí mật nhà nước trên phương tiện thông tin, viễn thông trái với quy định của pháp luật về cơ yếu.

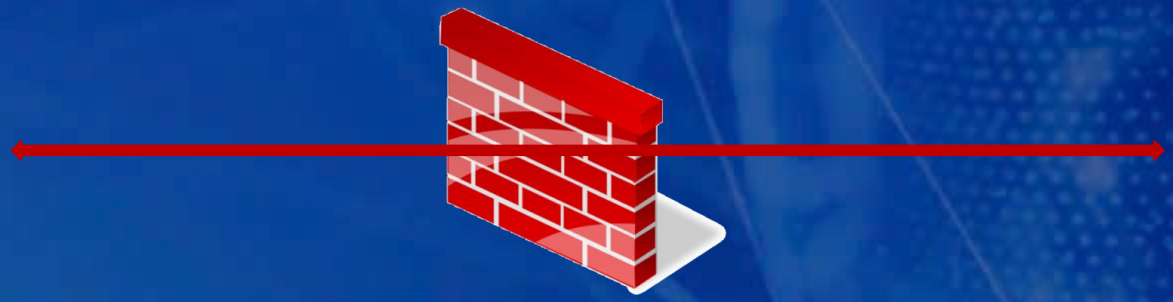
QUY ĐỊNH CỦA PHÁP LUẬT VỀ BẢO VỆ BMNN TRÊN KHÔNG GIAN MẠNG

Điều 5 Luật Bảo vệ bí mật nhà nước quy định các hành vi bị nghiêm cấm liên quan đến không gian mạng như sau:

- Chuyển mục đích sử dụng máy tính, thiết bị khác đã dùng để soạn thảo, lưu giữ, trao đổi bí mật nhà nước khi chưa loại bỏ bí mật nhà nước.
- Đăng tải, phát tán bí mật nhà nước trên phương tiện thông tin đại chúng, mạng Internet, mạng máy tính và mạng viễn thông.

NGUY CƠ TỪ LỖ HỔNG BẢO MẬT, VIRUS MÃ ĐỘC

- Máy tính tồn tại lỗ hổng bảo mật, tin tặc có thể khai thác từ xa.
- Máy tính nhiễm virus, mã độc đánh cắp thông tin truyền dữ liệu qua Internet.

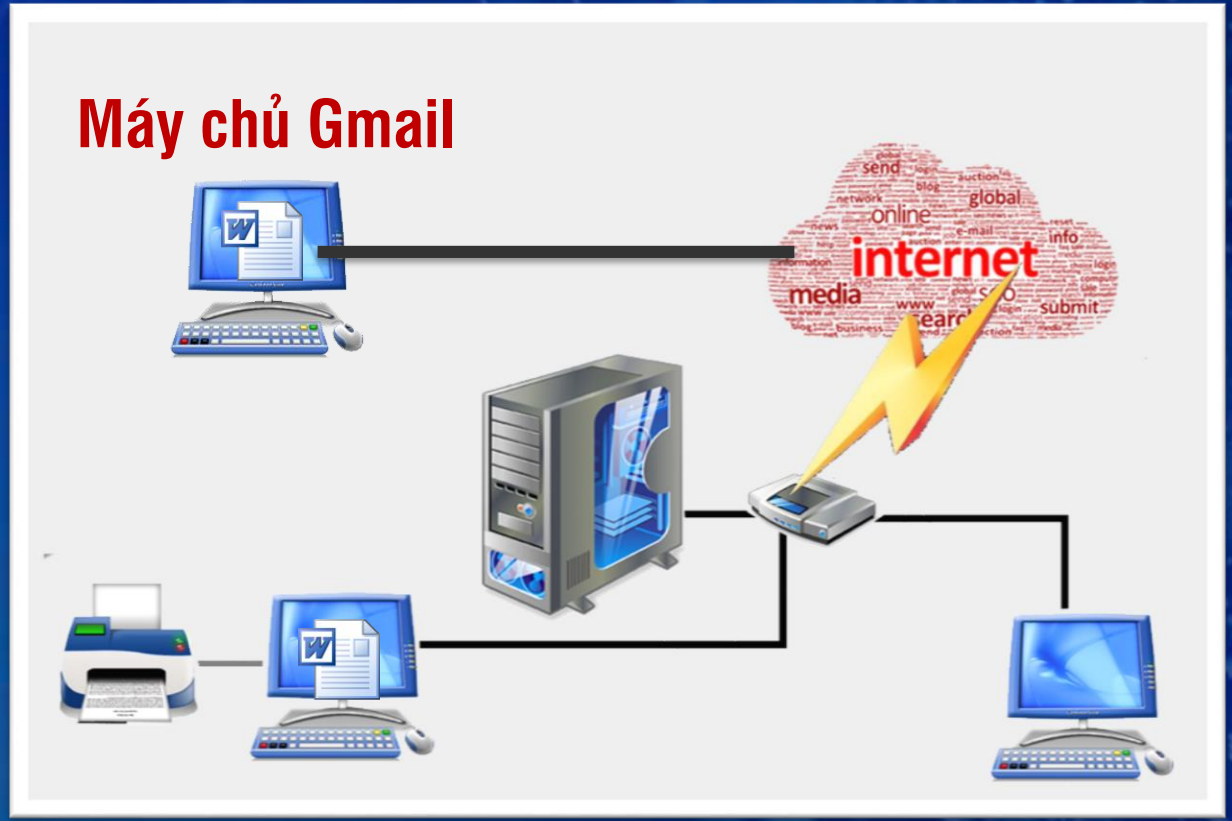


NGUY CƠ TỪ LỖ HỔNG BẢO MẬT, VIRUS MÃ ĐỘC

- **Nghiêm cấm** soạn thảo, lưu trữ tài liệu mang nội dung BMNN trên máy tính nối với mạng internet, mạng máy tính, mạng viễn thông.
- **Sử dụng** hệ điều hành mới (Windows 10 trở lên) và thường xuyên cập nhật bản vá lỗi.
- **Sử dụng** phần mềm Quét virus, mã độc có bản quyền; bật chế độ quét thường trực và thường xuyên cập nhật dữ liệu cho phần mềm (ít nhất 3 tháng).
- **Sử dụng** phần mềm tường lửa.

NGUY CƠ TỪ CÁC DỊCH VỤ TRÊN KHÔNG GIAN MẠNG

Nguy cơ lộ, lọt khi sử dụng thư điện tử công cộng.



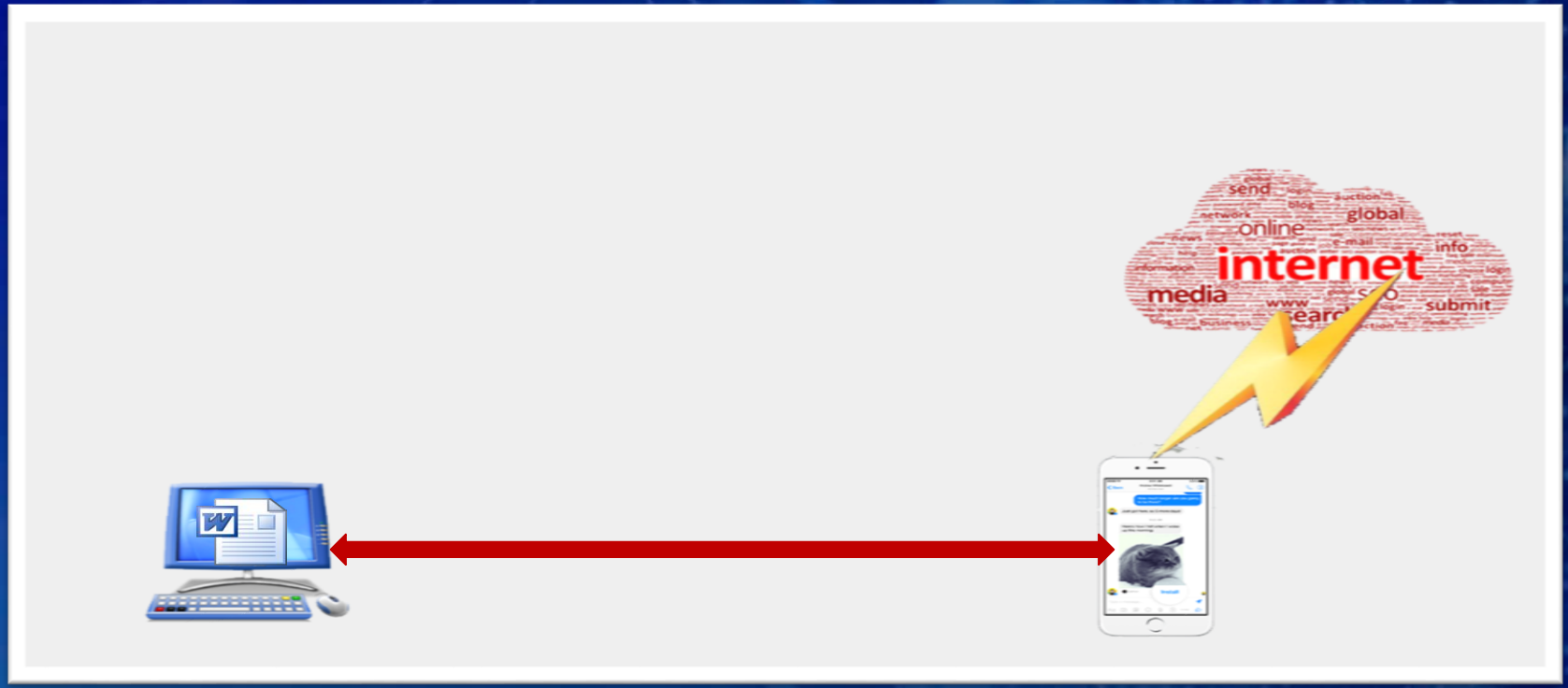
NGUY CƠ TỪ CÁC DỊCH VỤ TRÊN KHÔNG GIAN MẠNG

Nguy cơ lộ lọt khi gửi, nhận tài liệu qua các phần mềm OTT; sử dụng các dịch vụ lưu trữ tự động đồng bộ, sao lưu trên thiết bị; …

NGUY CƠ TỪ CÁC DỊCH VỤ TRÊN KHÔNG GIAN MẠNG

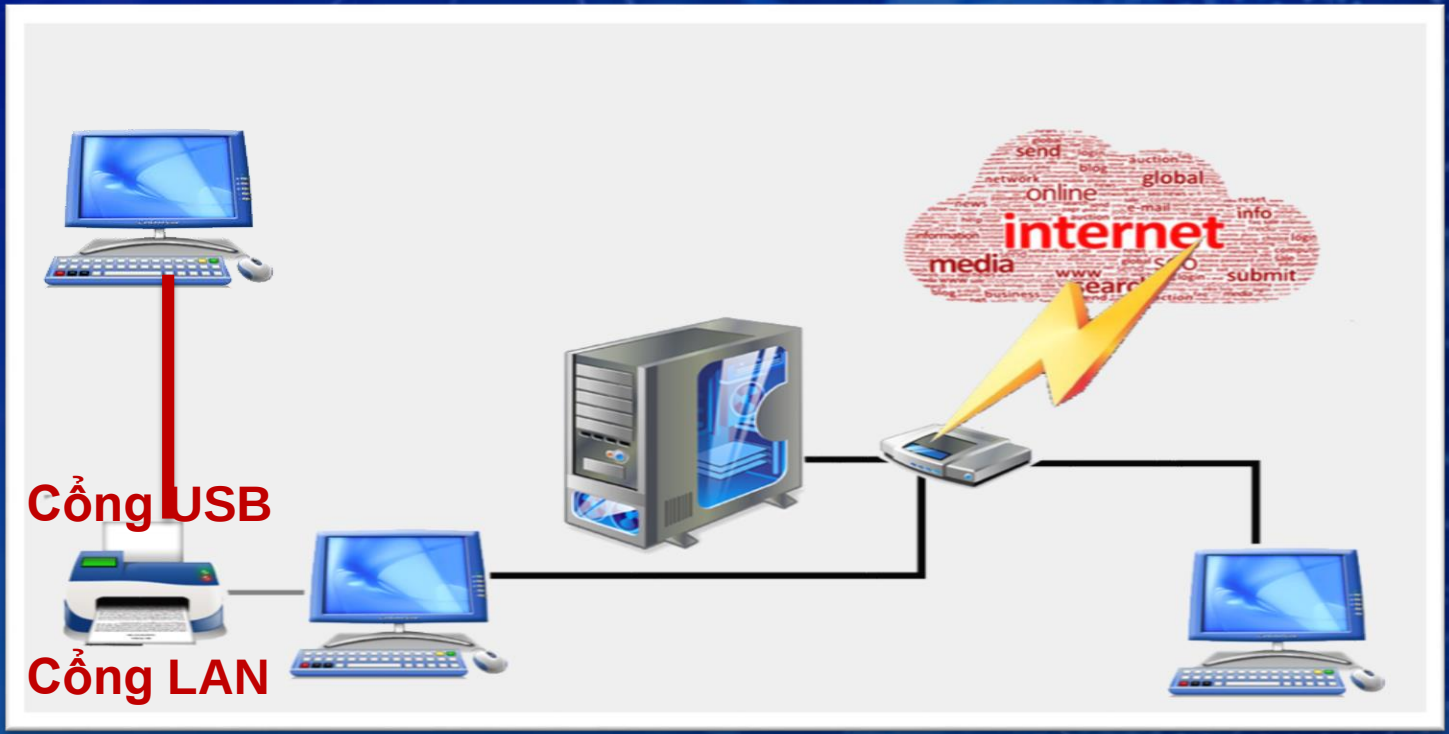
- **Nghiêm cấm** trao đổi, đăng tải nội dung BMNN qua mạng xã hội, hộp thư điện tử, trang thông tin điện tử, phương tiện thông tin đại chúng …
- **Nghiêm cấm** soạn thảo, chụp ảnh, lưu trữ nội dung BMNN trên điện thoại thông minh, máy tính bảng.

Nguy cơ khi kết nối các thiết bị có khả năng kết nối Internet vào máy tính độc lập, máy nối mạng riêng



Nghiêm cấm kết nối Internet, USB 3G, Wifi, điện thoại thông minh, máy tính bảng vào máy tính độc lập, máy nối mạng riêng.

Nguy cơ khi sử dụng máy in cùng lúc giữa máy tính độc lập và máy tính nối mạng internet



Nghiêm cấm sử dụng cùng lúc máy in giữa máy tính độc lập và máy tính nối mạng internet.

Nguy cơ khi photo tài liệu BMNN

- **Nghiêm cấm** photo tài liệu có nội dung **BMNN** bằng máy Photocopy ngoài quản lý của cơ quan
- **Format sạch** hoặc **tiêu hủy** ổ cứng khi dừng sử dụng

Nguy cơ do việc sử dụng chung USB giữa máy độc lập với máy tính nối mạng Internet (Mã độc Mustang Panda)

Nguy cơ do việc sử dụng chung USB giữa máy độc lập với máy tính nối mạng Internet (Mã độc Mustang Panda)

- Mã độc được gửi tới trong file nén (zip) để tránh bị chặn bởi các ứng dụng.
- Trong file nén có chứa file shortcut .lnk kèm theo đuôi .doc (ví dụ sample.doc.lnk) để đánh lừa người dung.

Nguy cơ do việc sử dụng chung USB giữa máy độc lập với máy tính nối mạng Internet (Mã độc Mustang Panda)

- **Cẩn trọng** khi tiếp nhận email, đường link, tệp tin lạ, xác thực chính xác nguồn gửi an toàn, đáng tin cậy.
- **Sử dụng** USB cơ yếu, bảo mật. Trước khi cắm USB vào máy Internet phải xóa sạch nội dung BMNN.

NGUY CƠ TỪ CHUYỂN MỤC ĐÍCH SỬ DỤNG MÁY TÍNH

- Tài liệu BMNN được soạn thảo trong quá trình sử dụng không được loại bỏ hoặc xóa bỏ không triệt để *(có thể phục hồi bằng các phần mềm chuyên dụng)*. Khi chuyển thành máy internet có nguy cơ bị đánh cắp dữ liệu.
- Trong quá trình sử dụng máy có khả năng bị nhiễm mã độc virus 0-day. Khi chuyển sang máy độc lập mã độc vẫn có khả năng đánh cắp dữ liệu *(phương thức hoạt động như mã độc Mustang Panda)*.

NGUY CƠ TỪ CHUYỂN MỤC ĐÍCH SỬ DỤNG MÁY TÍNH

- Cài đặt lại hệ điều hành và rà quét mã độc trước khi chuyển mục đích sử dụng.
- Đối với máy tính Độc lập, trước khi chuyển mục đích cần làm sạch dữ liệu theo tiêu chuẩn chống khôi phục (format từ 3-5 lần toàn bộ ổ cứng).

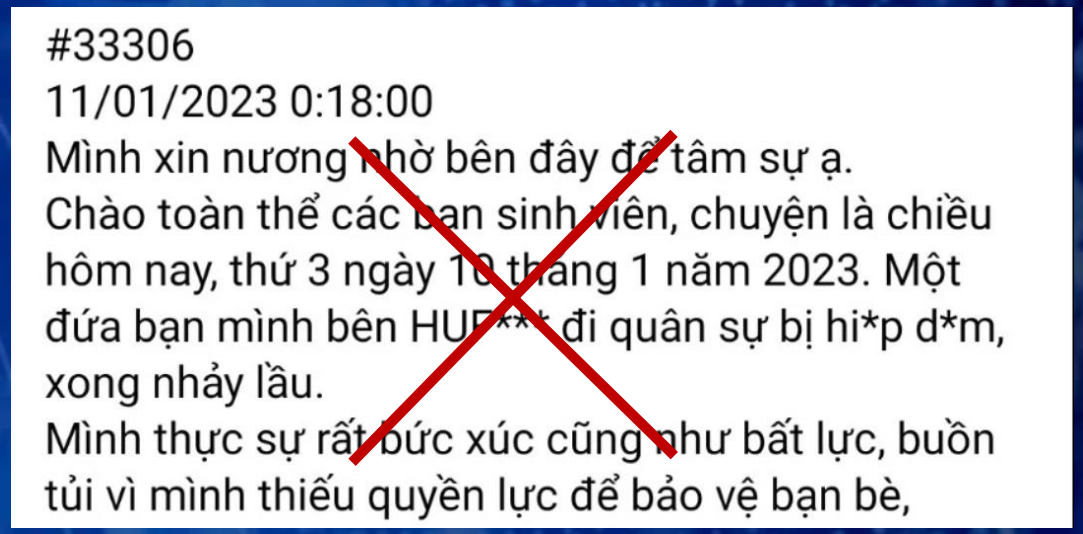
Phản bác, xử lý **thông tin xấu độc, sai sự thật**

“**Thông tin xấu độc, sai sự thật** là thông tin cố ý bịa đặt hoặc dùng thủ thuật lừa bịp bằng cách lan truyền qua phương tiện truyền thông hay mạng xã hội (MXH)."

Thông tin xấu độc, sai sự thật thường được tạo ra để tác động đến tư tưởng, quan điểm, tình cảm, cảm xúc, thái độ, hành vi của người dân, gây ảnh hưởng tiêu cực đến diễn biến thực tiễn, nhằm thực hiện các mục đích chính trị, lợi ích kinh tế hay ý đồ xấu xa của chủ thể tiến hành.

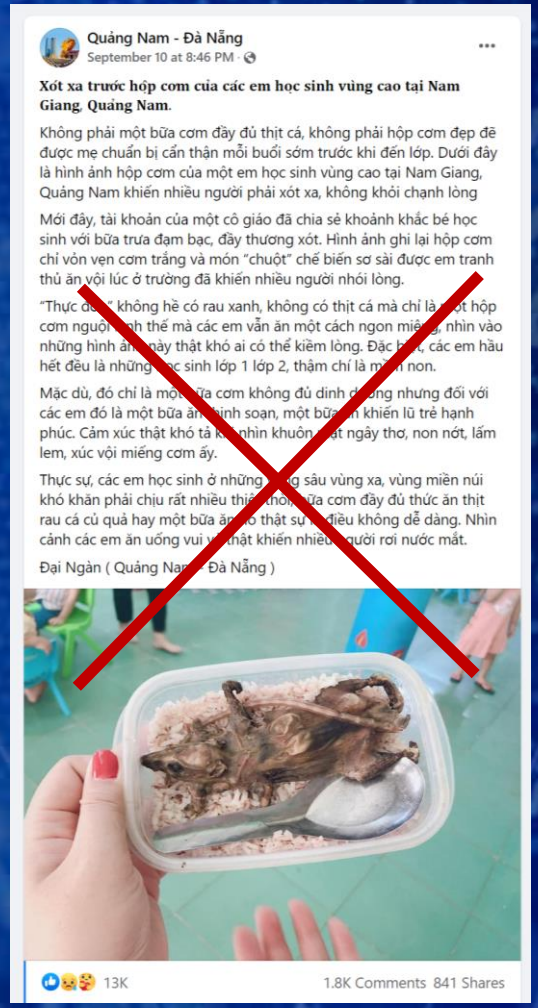
THÔNG TIN XẤU ĐỘC, SAI SỰ THẬT

Thông tin lan truyền hai nữ sinh HUFLIT bị xâm hại tình dục



THÔNG TIN XẤU ĐỘC, SAI SỰ THẬT

Thông tin về hộp cơm của các em học sinh vùng cao tại Nam Giang, Quảng Nam



THÔNG TIN XẤU ĐỘC, SAI SỰ THẬT

NHẬN DIỆN
THÔNG TIN XẤU ĐỘC, SAI SỰ THẬT

Thông tin xấu độc, sai sự thật

- **Nội dung tin** *(tìm kiếm Google, tin chính thống)*
- **Tài khoản đăng tải**
- **Hình ảnh** *(Google Lens)*
- **Căn cứ vào kiến thức bản thân**

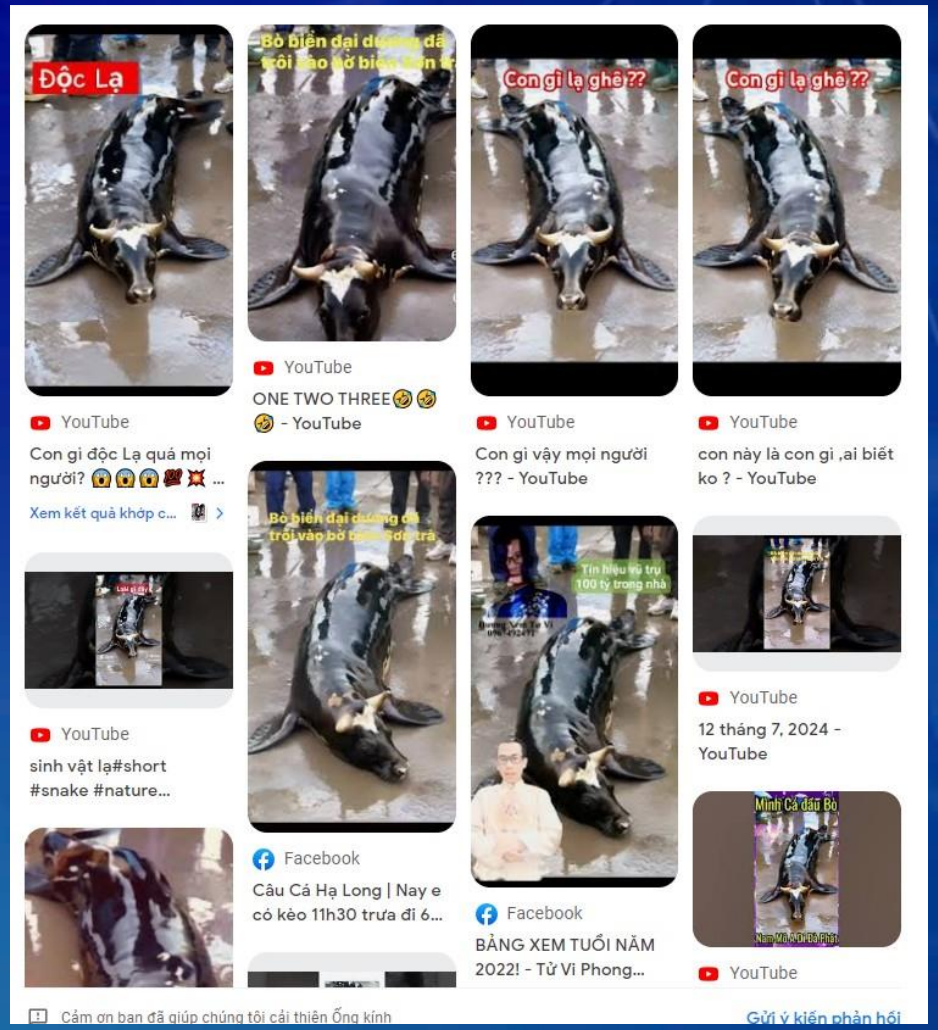
NHẬN DIỆN
THÔNG TIN XẤU ĐỘC, SAI SỰ THẬT

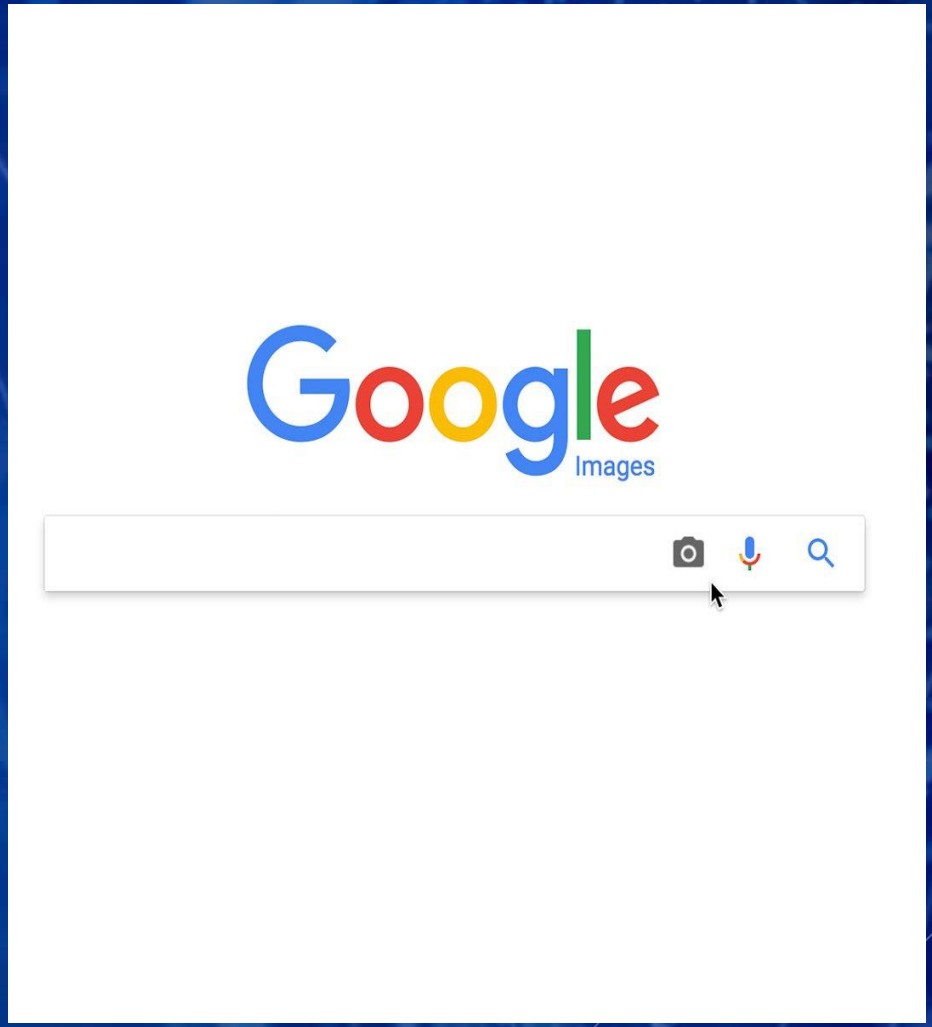
- Tiêu đề giật gân, thu hút, nội dung thông tin mới lạ, thường đề cập đến một vấn đề nóng đang được nhiều người quan tâm.
- Thông tin không ghi nguồn hoặc nguồn không rõ ràng.
- Thông tin xuất phát từ những trang web, tài khoản, kênh nội dung trên mạng xã hội thường xuyên tung tin giả, hoặc từ những trang, tài khoản, kênh không thuộc cơ quan báo chí chính thống hoặc cơ quan nhà nước.

NHẬN DIỆN
THÔNG TIN XẤU ĐỘC, SAI SỰ THẬT

- Xem xét nguồn tin, kiểm tra tác giả.
- Kiểm tra thông tin, hình ảnh minh họa và đường dẫn liên kết.
- Kiểm tra thời gian.
- Đọc toàn bộ nội dung, tìm những điểm nghi ngờ, mâu thuẫn.
- Đối chiếu với thông tin trên báo chí chính thống hoặc tham khảo ý kiến chuyên gia hoặc các cơ quan chức năng.

NHẬN DIỆN
THÔNG TIN XẤU ĐỘC, SAI SỰ THẬT





CÁCH XỬ LÝ
THÔNG TIN XẤU ĐỘC, SAI SỰ THẬT

Các bước cần làm khi thấy tin giả:

- Lưu lại bằng chứng (lưu lại đường link, chụp ảnh màn hình tin, bài viết nghi là tin giả, tải video nghi là tin giả về máy tính, điện thoại của mình...).
- Không chia sẻ và cảnh báo cho người thân, bạn bè không chia sẻ những thông tin nghi ngờ là giả này.
- Cảnh báo cho người đang đăng tải, chia sẻ những thông tin này về khả năng họ đang lan truyền tin giả và hậu quả của việc này.
- Thông báo tin giả đến cơ quan chức năng có thẩm quyền.

CÁCH XỬ LÝ
THÔNG TIN XẤU ĐỘC, SAI SỰ THẬT

Trung tâm Xử lý tin giả Việt Nam (VAFC) thuộc Cục Phát thanh, truyền hình và thông tin điện tử (Bộ Thông tin và Truyền thông) thông qua các phương thức sau:

Website: https://tingia.gov.vn;

Email: online.abei@mic.gov.vn;

Hotline: 18008108.

TÌNH HÌNH
AN NINH MẠNG

Trên Thế giới, tại Việt Nam và thành phố Đà Nẵng

8 000 000 000 000 USD

tương đương gần 196 triệu tỷ VNĐ
là thiệt hại bởi các vụ tấn công mạng

Các mục tiêu mềm dễ tấn công

Như các viện nghiên cứu, tổ chức phi chính phủ và các trường đại học, vẫn là các mục tiêu hàng đầu.

Nâng cao khả năng tiếp cận

Các mục tiêu khó tấn công như quan chính phủ hay ngành công nghiệp quốc phòng.

Sự cố màn hình xanh ngày 19/7

"**Việt Nam** đứng đầu trong top 10 quốc gia có số lượng mục tiêu bị tấn công bởi phần mềm độc hại Infostealer tại khu vực Châu Á Thái Bình Dương năm 2023."

Theo nghiên cứu của Cyberint

8.168

cuộc tấn công lừa đảo

451

cuộc tấn công thay đổi nội dung website

884

cuộc tấn công mã độc

TẤN CÔNG RANSOMWARE TẠI VIỆT NAM

VNDirect

24/03/2024

PVOIL

02/04/2024

Nhiều cá nhân, tổ chức, cơ quan, đơn vị khác ...

NGUY CƠ ĐE DỌA AN NINH MẠNG TẠI THÀNH PHỐ

- Sở Thông tin và Truyền thông ghi nhận, ngăn chặn **3.228 lượt tấn công** vào các hệ thống thông tin của thành phố.
- Công an thành phố phát hiện, hướng dẫn xử lý **nhiều nguy cơ đe dọa / sự cố an ninh mạng**.

Nổi lên:

- Sự cố Trung tâm Công nghệ thông tin thuộc Sở Tài nguyên Môi trường bị tấn công mã độc mã hóa tống tiền vào tháng 5/2024.

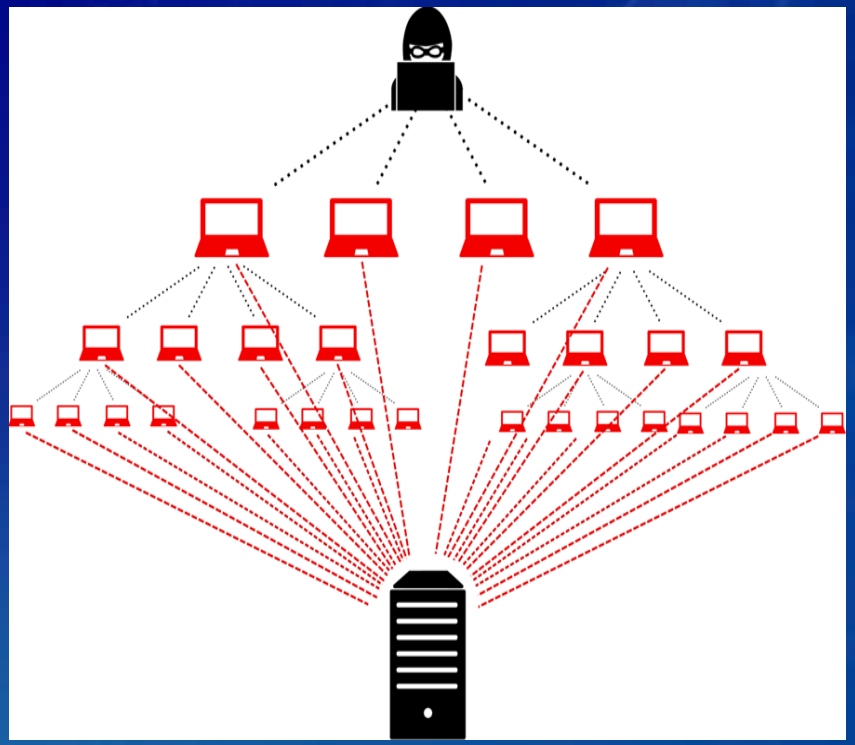
- Các trang thông tin điện tử của cơ quan, đơn vị bị đặt backlink quảng cáo trái phép và lộ, lọt tài khoản quản trị các hệ thống thông tin.

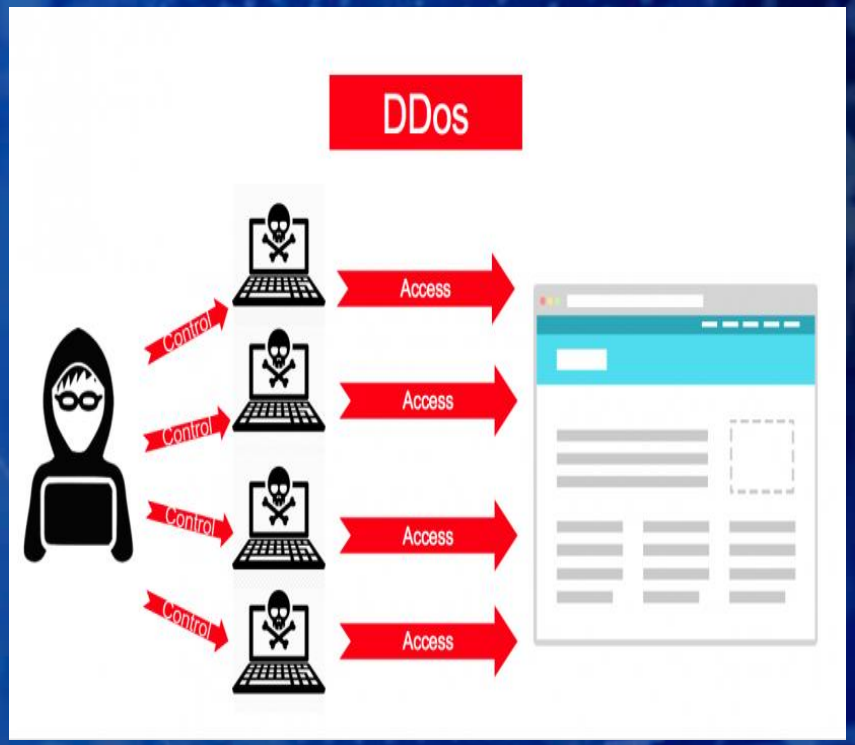
Một số hình thức **tấn công mạng**

"**Tấn công mạng** là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để phá hoại, gây gián đoạn hoạt động của 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, phương tiện điện tử."

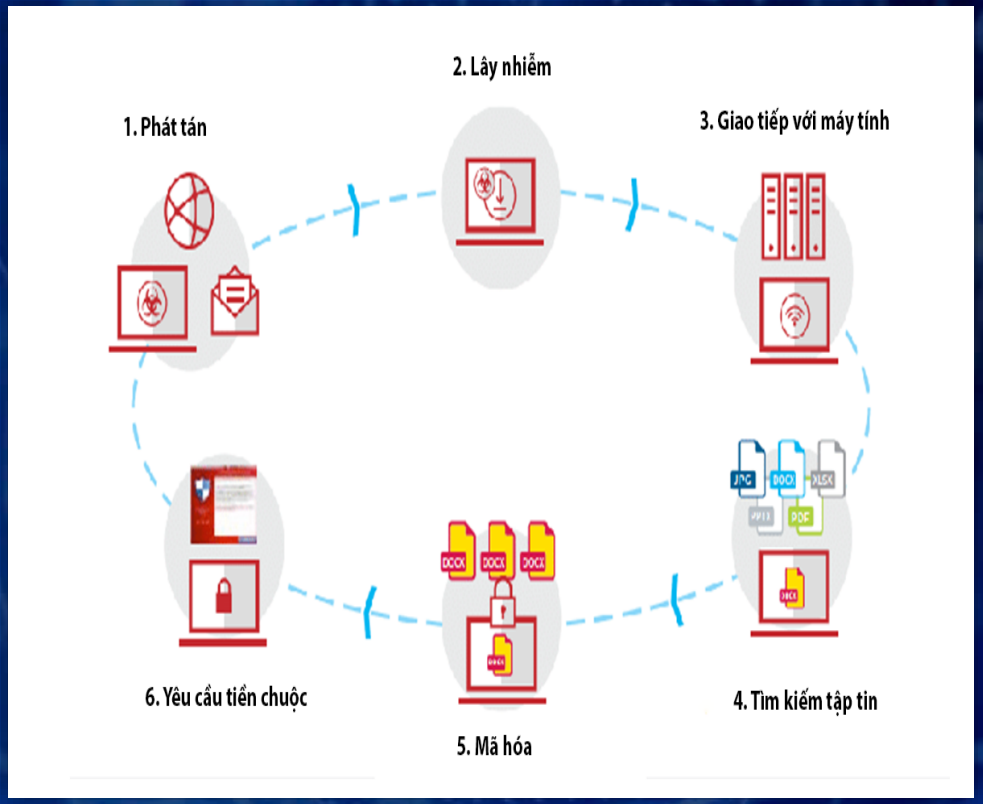
Theo khoản 8 Điều 2 Luật An ninh mạng 2018

TẤN CÔNG DDOS



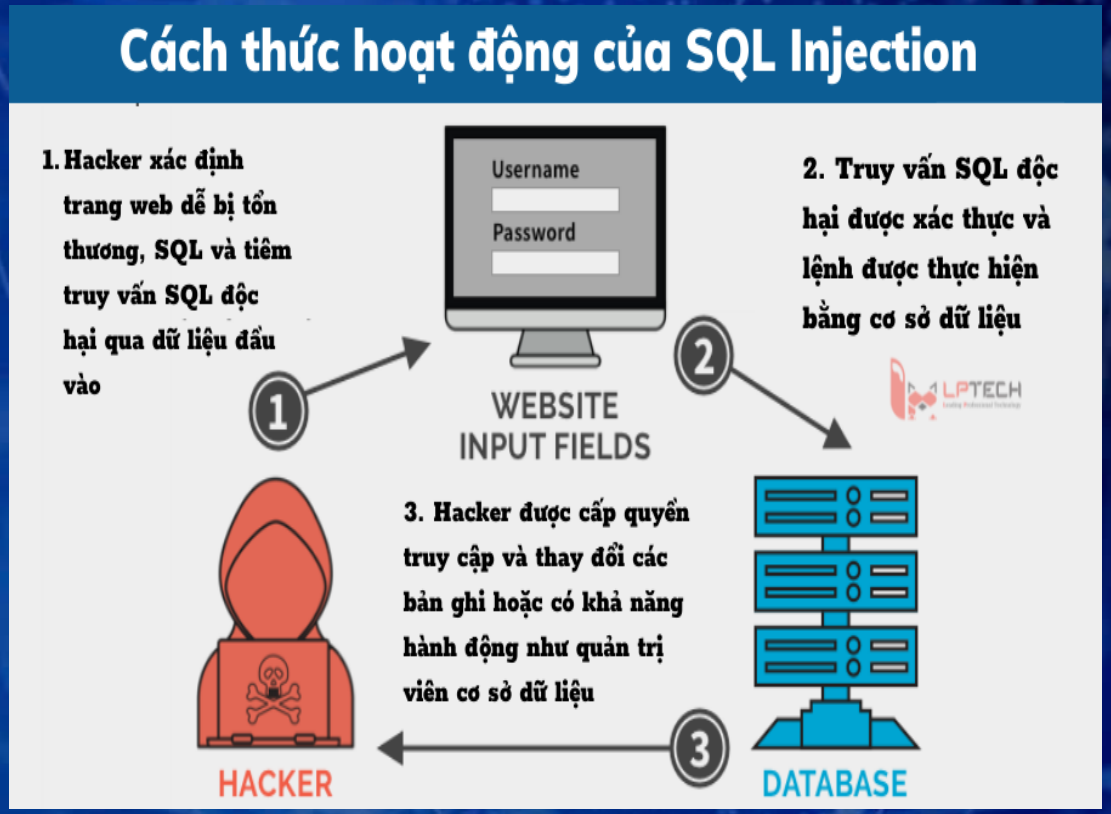


TẤN CÔNG MÃ ĐỘC



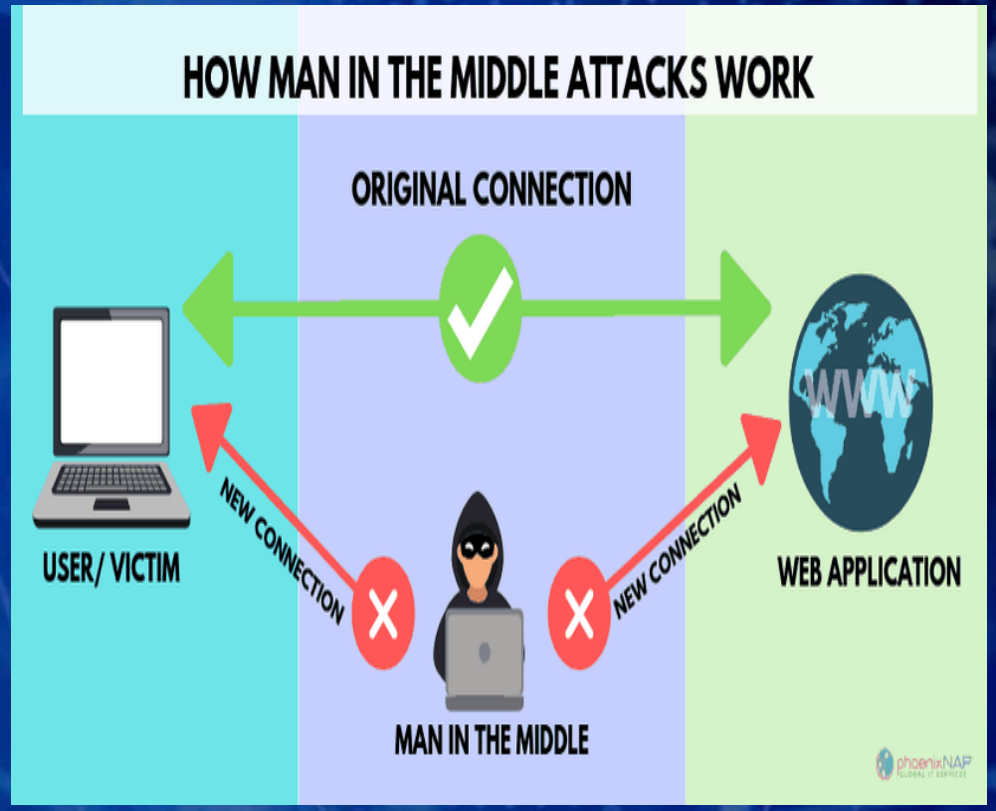
TẤN CÔNG SQL INJECTION

Là một kỹ thuật cho phép kẻ tấn công chèn mã SQL vào dữ liệu gửi đến máy chủ và cuối cùng được thực hiện trên máy chủ cơ sở dữ liệu.

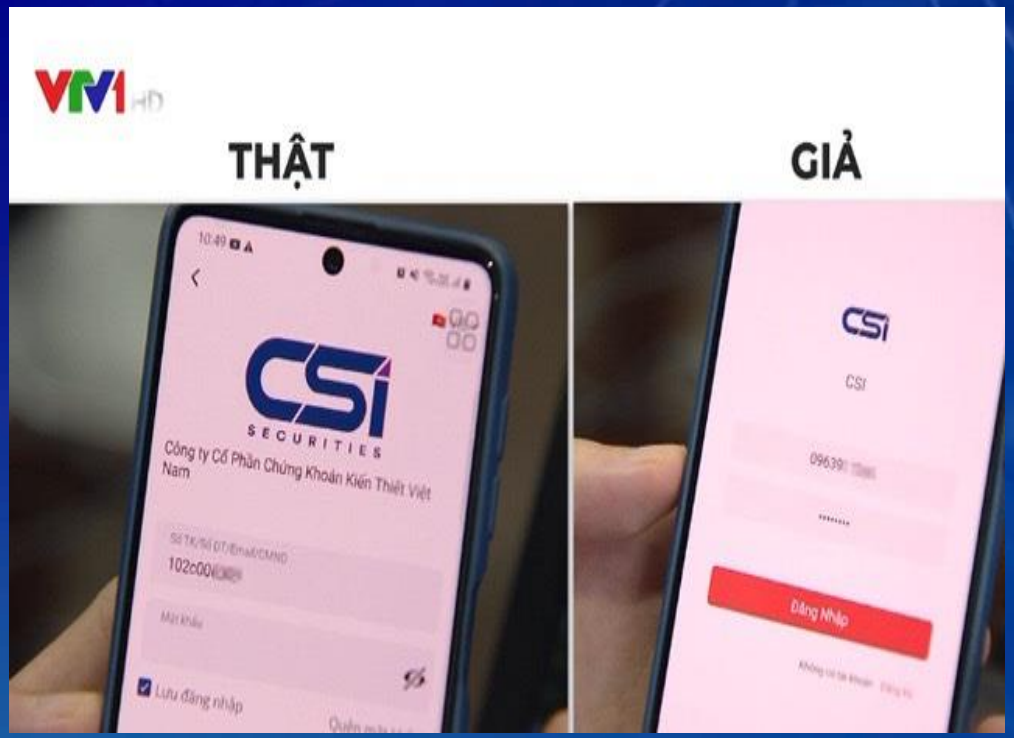


TẤN CÔNG MAN-IN-THE-MIDDLE

Là một loại tấn công mạng mà hacker sẽ đứng giữa người dùng và ứng dụng. Kẻ tấn công sẽ chặn và và kiểm soát toàn bộ quá trình giao tiếp giữa hai bên để người dùng tin rằng họ vẫn đang trực tiếp liên lạc với nhau.

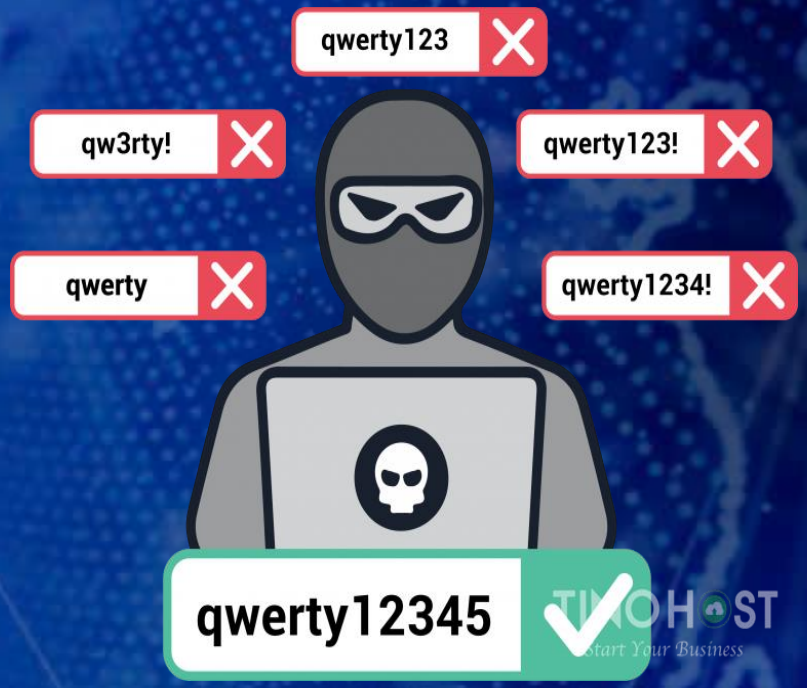


TẤN CÔNG PHISHING



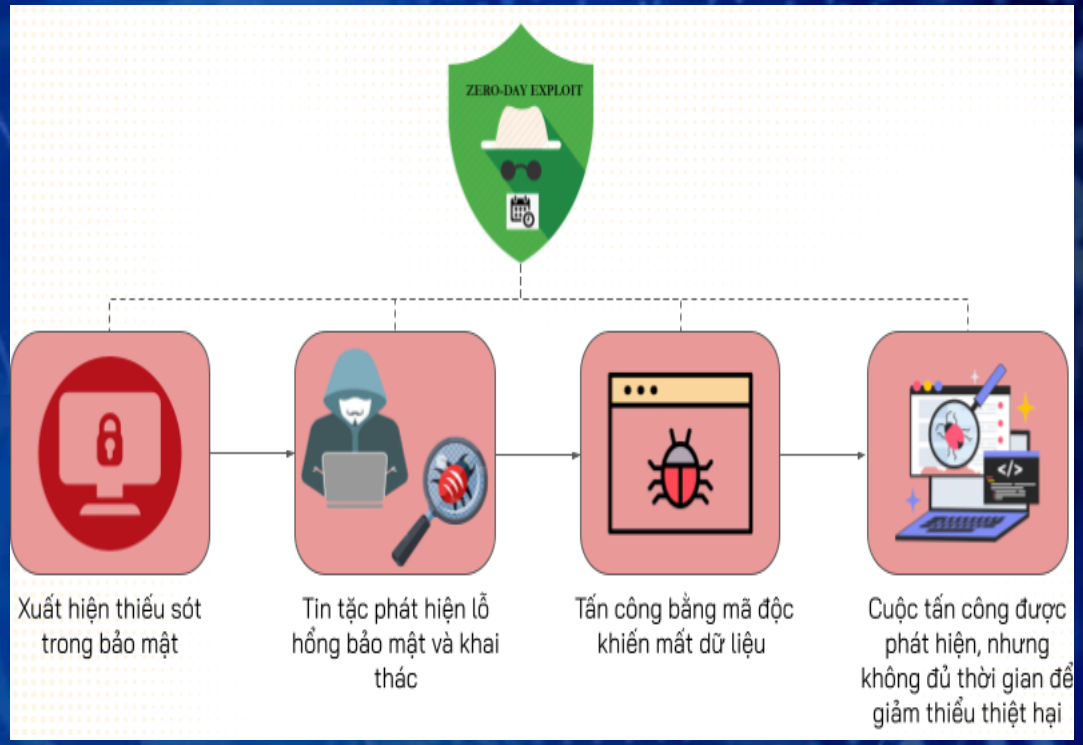
TẤN CÔNG MẬT KHẨU

- Tấn công dò mật khẩu
- Tấn công từ điển
- Tấn công Key Logger

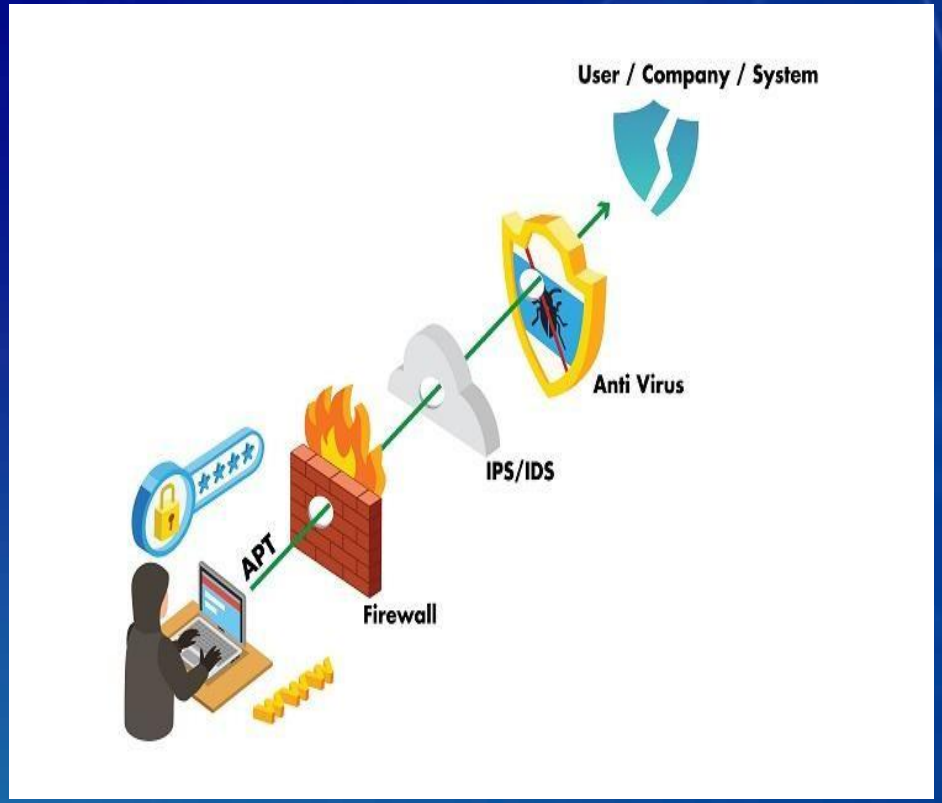


TẤN CÔNG KHAI THÁC LỖ HỔNG

Trong lĩnh vực an ninh mạng, lỗ hổng bảo mật là một điểm yếu có thể bị khai thác bởi một tác nhân xấu để thực hiện các cuộc tấn công mạng nhằm mục đích thực hiện các hành động phi pháp lên hệ thống mục tiêu.



TẤN CÔNG APT


User / Company / System
Anti Virus
IPS/IDS
APT
Firewall


Xác định mục đích tấn công
Tìm kiếm mục tiêu phù hợp
Chế tạo công cụ tấn công
Nghiên cứu về Con người/Hạ tầng của mục tiêu
Thử
Triển khai
Khởi tạo việc xâm nhập
Khởi sinh kết nối từ bên ngoài
Mở rộng ảnh hưởng
Đánh cắp định danh
Đánh cắp dữ liệu
Xóa dấu vết

Các phương thức, thủ đoạn **lừa đảo**

"**Tội phạm mạng** là hành vi sử dụng không gian mạng, công nghệ thông tin hoặc phương tiện điện tử để thực hiện tội phạm được quy định tại Bộ luật Hình sự."

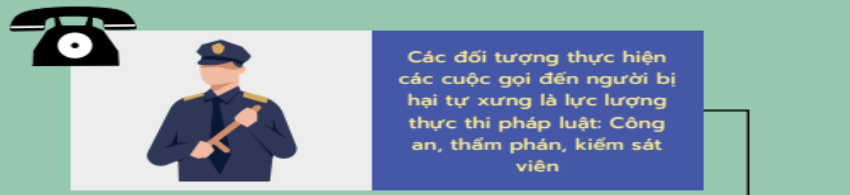
Theo khoản 74 Điều 2 Luật An ninh mạng 2018

Giả danh Công an, Viện kiểm sát,...

Công an TP Đà Nẵng
Phòng ANM&PCTPSDCNC

THÔNG BÁO PHƯƠNG THỨC THỦ ĐOẠN LỪA ĐẢO CHIẾM ĐOẠT TÀI SẢN

Tự xưng cơ quan chức năng gọi điện thông báo điều tra



Các đối tượng thực hiện các cuộc gọi đến người bị hại tự xưng là lực lượng thực thi pháp luật: Công an, thẩm phán, kiểm sát viên

Thông báo người bị hại có liên quan đến các hành vi vi phạm pháp luật như: gây tai nạn, buôn bán ma túy,...

Làm giả các lệnh truy nã, quyết định khởi tố, lệnh bắt gửi đến người bị hại. Sau đó yêu cầu bị hại thực hiện một trong hai cách sau:

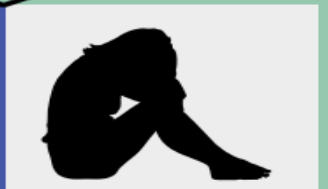
Chuyển hết tiền vào tài khoản theo yêu cầu của đối tượng để phục vụ "điều tra xác minh" tài sản

Cài phần mềm "Bộ công an" vào điện thoại để phục vụ "công tác điều tra", thực chất là để chiếm quyền sử dụng điện thoại

Đối tượng sau đó nhanh chóng chuyển tiền zíc zắc qua nhiều tài khoản khác nhau nhằm cắt đứt thông tin dòng tiền

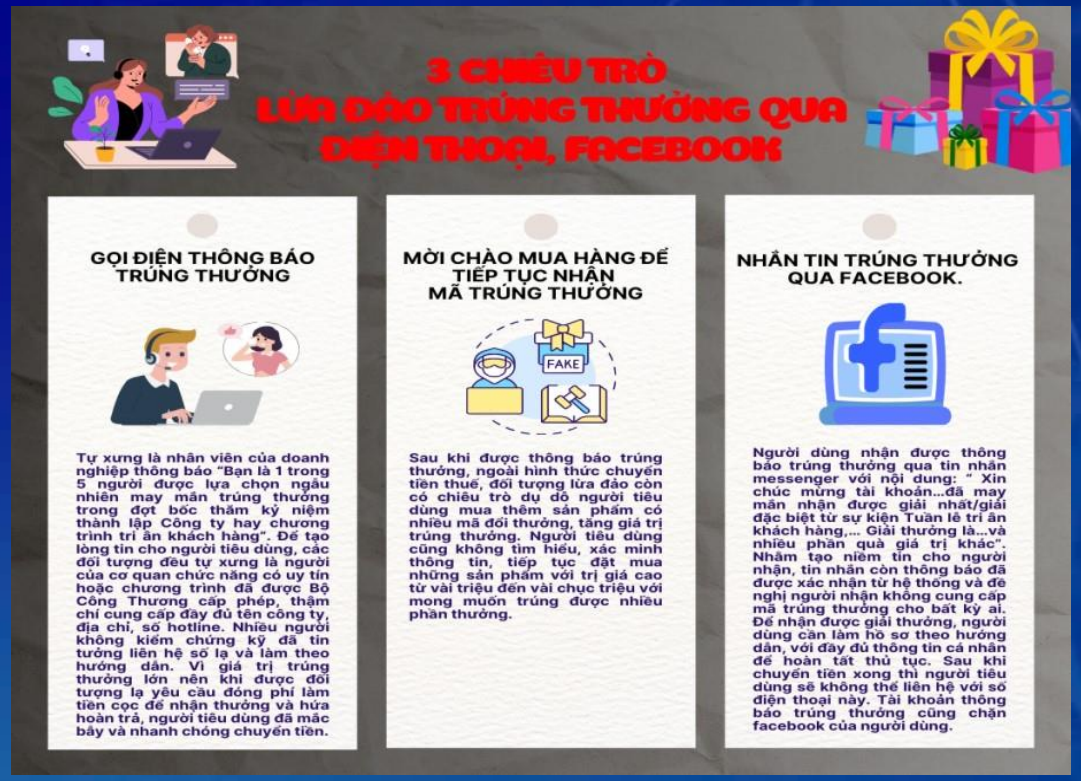
Đối tượng sau đó nhanh chóng chuyển tiền trong tài khoản ngân hàng của nạn nhân qua tài khoản ngân hàng của đối tượng

Khi bị hại phát hiện ra mình bị lừa thì đã quá muộn do dòng tiền lúc này đã được chuyển sang rất nhiều lớp tài khoản ngân hàng khác nhau.

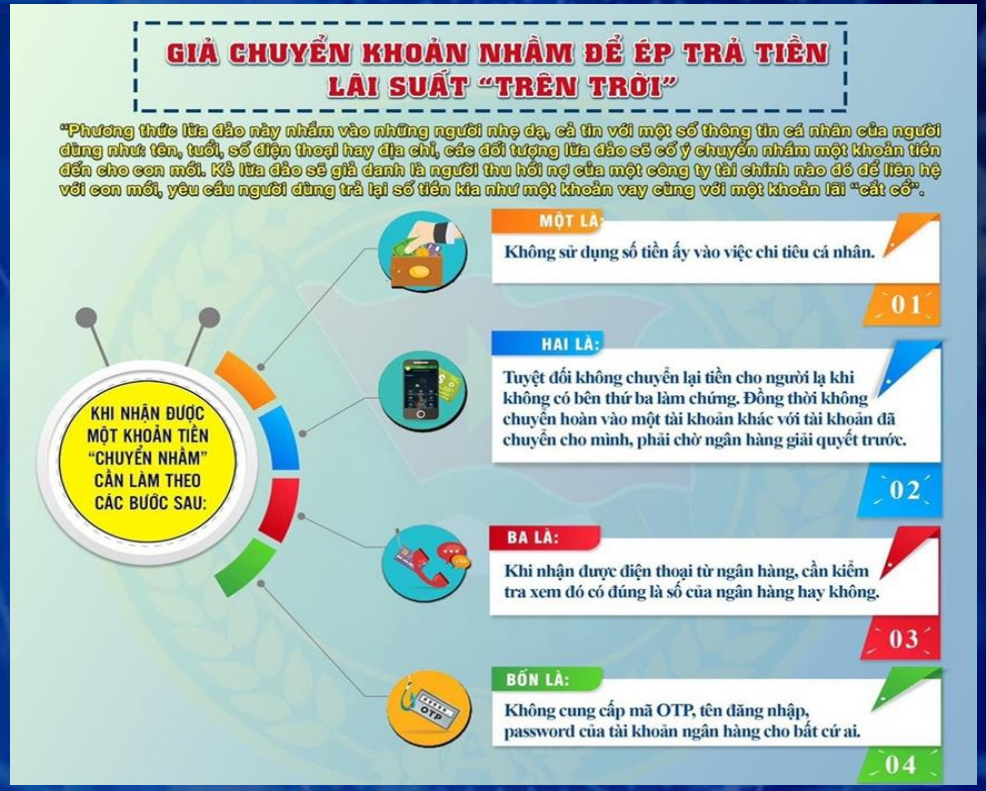


Bài học rút ra: Cơ quan chức năng không bao giờ làm việc qua điện thoại, không bao giờ yêu cầu chuyển tiền vào tài khoản cá nhân, tổ chức để xác minh điều tra

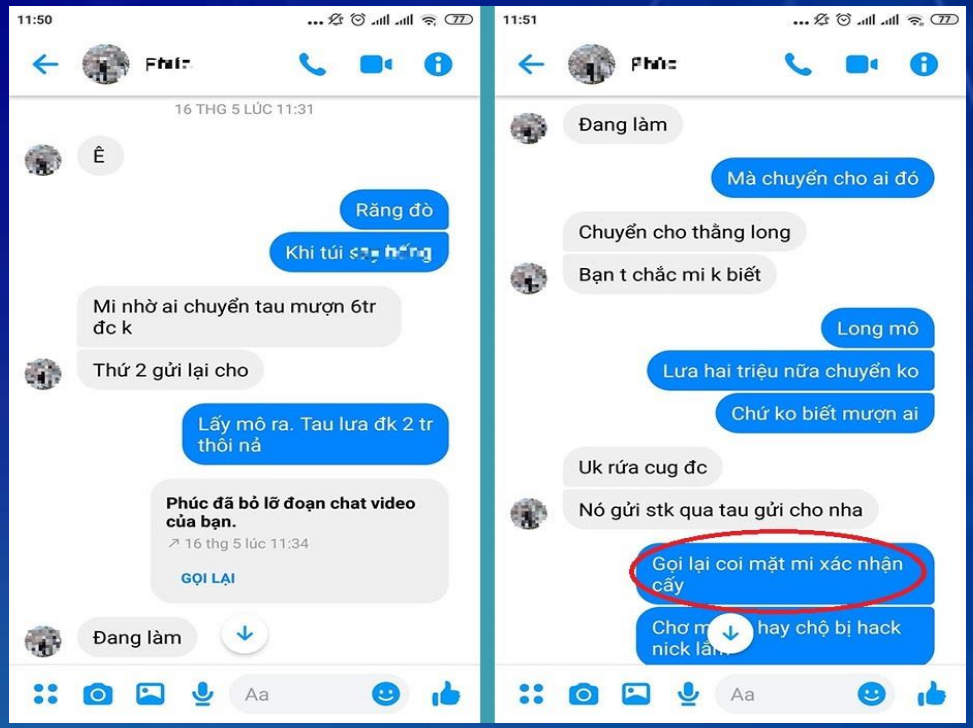
Thông báo trúng thưởng



Chuyển nhầm tiền vào tài khoản



Đánh cắp tài khoản Facebook để mượn tiền



Tuyển dụng cộng tác viên online

Lừa đảo bằng Deepfake


Personal Data
Name
Home Address
Business Address
Identity Card No
Passport No
Driving License
Income Tax No
Car Registration
Other
Confidential Data
data privacy
[Identify Person]

DỮ LIỆU CÁ NHÂN

Dữ liệu cá nhân là thông tin dưới dạng ký hiệu, chữ viết, chữ số, hình ảnh, âm thanh hoặc dạng tương tự trên môi trường điện tử gắn liền với một con người cụ thể hoặc giúp xác định một con người cụ thể. Dữ liệu cá nhân bao gồm dữ liệu cá nhân cơ bản và dữ liệu cá nhân nhạy cảm

Khoản 1 Điều 2

BẢO VỆ DỮ LIỆU CÁ NHÂN

Bảo vệ dữ liệu cá nhân là hoạt động phòng ngừa, phát hiện, ngăn chặn, xử lý hành vi vi phạm liên quan đến dữ liệu cá nhân theo quy định của pháp luật

Khoản 5 Điều 2

Hoạt động thu thập dữ liệu cá nhân của cơ quan nhà nước, tổ chức, doanh nghiệp, cá nhân với chủ thể dữ liệu

- Thứ nhất, nhận thức chưa đầy đủ về trách nhiệm bảo vệ DLCN nên từ đó chủ quan, không chú ý một cách đầy đủ các giải pháp bảo vệ DLCN trong khi thủ đoạn, cách thức tấn công mạng ngày càng tinh vi, phức tạp.
- Thứ hai, hệ thống bảo mật của các doanh nghiệp, đặc biệt là các doanh nghiệp vừa và nhỏ, hiện còn rất hạn chế, thậm chí có doanh nghiệp còn trong tình trạng sơ sài, yếu kém.

Hoạt động thu thập dữ liệu cá nhân của cơ quan nhà nước, tổ chức, doanh nghiệp, cá nhân với chủ thể dữ liệu

- Thứ ba, chưa có một quy trình bảo vệ DLCN chuẩn trong doanh nghiệp, do vậy khả năng dò rỉ DLCN xuất phát từ chính con người vận hành hệ thống.
- Thứ tư, từ góc độ quản lý nhà nước chưa có một cơ quan chuyên trách về bảo vệ dữ liệu để đưa ra các yêu cầu tối thiểu đảm bảo an ninh bảo mật cả về công nghệ cũng như quy trình và giám sát việc tuân thủ.

Hoạt động thu thập dữ liệu cá nhân của cơ quan nhà nước, tổ chức, doanh nghiệp, cá nhân với chủ thể dữ liệu

- Thứ năm là nhân lực an ninh mạng. Chúng ta thiếu và yếu cả nhân lực vận hành cũng như doanh nghiệp cung cấp giải pháp. Nhân lực đảm bảo an ninh mạng ở các doanh nghiệp vừa và nhỏ đa số là kiêm nhiệm, kiến thức và kỹ năng an ninh, an ninh không gian mạng không được cập nhật, trong khi thủ đoạn tấn công mạng lại càng tinh vi phức tạp.

Hoạt động thu thập dữ liệu cá nhân từ tội phạm công nghệ cao (tổ chức, cá nhân) với chủ thể dữ liệu

Phương thức, thủ đoạn thu thập trái phép dữ liệu cá nhân:

- Thông qua các Website
- Thông qua phần mềm miễn phí
- Thông qua hòm thư điện tử
- Tấn công thông qua vật trung gian
- Tấn công qua các thiết bị thông minh

Hoạt động thu thập dữ liệu cá nhân từ tội phạm công nghệ cao (tổ chức, cá nhân) với chủ thể dữ liệu

Đối tượng thu thập trái phép dữ liệu cá nhân:

- Tấn công nội bộ
- Tấn công từ bên ngoài

Hoạt động xử lý dữ liệu cá nhân của Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên Kiểm soát và Xử lý dữ liệu cá nhân, Bên thứ ba với chủ thể dữ liệu

- Xác định các yêu cầu bảo mật
- Hoạt động thẩm tra

Hoạt động xử lý dữ liệu cá nhân giữa cá nhân với cá nhân

- Đặt mật khẩu yếu
- Lỗ hổng từ các phần mềm, cửa hậu
- Phần mềm độc hại
- Kỹ thuật tấn công phi kỹ thuật (Social engineering attack)
- Sự bất cẩn của người dùng
- Chia sẻ dữ liệu cá nhân quá nhiều trên các phương tiện truyền thông xã hội
- Chủ quan trong tham gia ký kết các điều khoản giao dịch

Chế tài xử phạt hành vi xâm phạm dữ liệu cá nhân

- Chế tài hình sự: Vi phạm các quy định về dữ liệu cá nhân có thể bị xử phạt hình sự, với án tù giam cao nhất là 07 năm. Cụ thể: Điều 159 Bộ Luật Hình sự quy định, việc "xâm phạm bí mật hoặc an ninh thư tín, điện thoại, điện tín hoặc hình thức trao đổi thông tin riêng tư của người khác" có thể bị phạt tù tới 03 năm. Điều 288 quy định về "Tội đưa hoặc sử dụng trái phép thông tin trên mạng máy tính, mạng viễn thông" với mức hình phạt cao nhất là 07 năm tù giam.

Chế tài xử phạt hành vi xâm phạm dữ liệu cá nhân

- Chế tài dân sự: Quyền bảo vệ dữ liệu cá nhân (dữ liệu cá nhân) là một quyền dân sự, việc bảo vệ quyền này được coi là nguyên tắc trong pháp luật Dân sự. Khoản 1 Điều 9 Bộ luật Dân sự năm 2015 khẳng định: “Tất cả các quyền dân sự của cá nhân, pháp nhân, chủ thể khác được tôn trọng và được pháp luật bảo vệ”.

Chế tài xử phạt hành vi xâm phạm dữ liệu cá nhân

- Chế tài hành chính: Các hành vi vi phạm, xâm hại đến dữ liệu cá nhân có thể bị buộc bồi thường thiệt hại, xử phạt vi phạm hành chính hoặc truy cứu trách nhiệm hình sự, tùy thuộc vào tính chất, mức độ nguy hiểm và hậu quả do hành vi vi phạm gây ra.

Thực trạng dữ liệu cá nhân đang bị mua bán, lộ, mất tràn lan

Thực trạng dữ liệu cá nhân đang bị mua bán, lộ, mất tràn lan

- Chỉ trong 02 năm từ năm 2019 đến năm 2020, 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 1.300GB, trong đó có nhiều dữ liệu cá nhân nội bộ, nhạy cảm.

Kết quả đấu tranh, phòng chống vi phạm pháp luật về bảo vệ dữ liệu cá nhân trên địa bàn TP Đà Nẵng

Đánh sập 2 đường dây chuyên mua bán dữ liệu cá nhân, sim rác, tạo và mua bán tài khoản ngân hàng số lượng lớn


THDT1
THỜI SỰ

Kết quả công tác bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu

- Lỗ hổng API tra cứu giấy phép lái xe của Sở Giao thông vận tải có thể bị lợi dụng để thu thập 486.653 giấy phép lái xe, thông tin dữ liệu cá nhân bao gồm: họ tên, số chứng mình nhân dân, ngày sinh, địa chỉ.
- Lỗ hổng API tra cứu thông tin khách hàng của Công ty Cổ phần cấp nước Đà Nẵng có thể bị lợi dụng để thu thập 340.238 thông tin khách hàng, thông tin dữ liệu cá nhân bao gồm: họ tên, địa chỉ, số điện thoại.

Kết quả công tác bảo vệ dữ liệu cá nhân trong quá trình xử lý dữ liệu

- Lỗ hổng bảo mật nghiêm trọng CVE-2019-16891, CVE-2020-7961 tại 39 trang thông tin điện tử sử dụng nền tảng Liferay Portal của các đơn vị trên địa bàn thành phố có thể bị khai thác để tấn công chiếm quyền điều khiển đánh cắp dữ liệu trên máy chủ, có nguy cơ lộ lọt dữ liệu cá nhân của cán bộ, viên chức được lưu trên hệ thống.

NGUYÊN TẮC BẢO VỆ DỮ LIỆU CÁ NHÂN

1. Dữ liệu cá nhân được xử lý theo quy định của pháp luật.
2. Chủ thể dữ liệu được biết về hoạt động liên quan tới xử lý dữ liệu cá nhân của mình, trừ trường hợp luật có quy định khác.
3. Dữ liệu cá nhân chỉ được xử lý đúng với mục đích đã được Bên Kiểm soát dữ liệu cá nhân, Bên Xử lý dữ liệu cá nhân, Bên Kiểm soát và xử lý dữ liệu cá nhân, Bên thứ ba đăng ký, tuyên bố về xử lý dữ liệu cá nhân.

NGUYÊN TẮC BẢO VỆ DỮ LIỆU CÁ NHÂN

4. Dữ liệu cá nhân thu thập phải phù hợp và giới hạn trong phạm vi, mục đích cần xử lý. Dữ liệu cá nhân không được mua, bán dưới mọi hình thức, trừ trường hợp luật có quy định khác.

5. Dữ liệu cá nhân được cập nhật, bổ sung phù hợp với mục đích xử lý.

6. Dữ liệu cá nhân được áp dụng các biện pháp bảo vệ, bảo mật trong quá trình xử lý, bao gồm cả việc bảo vệ trước các hành vi vi phạm quy định về bảo vệ dữ liệu cá nhân và phòng, chống sự mất mát, phá hủy hoặc thiệt hại do sự cố, sử dụng các biện pháp kỹ thuật.

NGUYÊN TẮC BẢO VỆ DỮ LIỆU CÁ NHÂN

7. Dữ liệu cá nhân chỉ được lưu trữ trong khoảng thời gian phù hợp với mục đích xử lý dữ liệu, trừ trường hợp pháp luật có quy định khác.

8. Bên Kiểm soát dữ liệu, Bên Kiểm soát và xử lý dữ liệu cá nhân phải chịu trách nhiệm tuân thủ các nguyên tắc xử lý dữ liệu được quy định từ khoản 1 tới khoản 7 Điều này và chứng minh sự tuân thủ của mình với các nguyên tắc xử lý dữ liệu đó.

Biện pháp **an toàn** trên không gian mạng

Biện pháp **an toàn** trên không gian mạng

Biện pháp **an toàn** trên không gian mạng

HÃY

- Mạnh mẽ
- Thông thái
- Cảnh giác
- Tử tế
- Dũng cảm

HÃY MẠNH MẼ

Một trong những bí kíp hiệu quả giúp chúng mình được an toàn hơn trên môi trường mạng đó là đảm bảo mật khẩu của các tài khoản cá nhân có tính bảo mật cao. Cùng nhau nắm rõ 5 bí kíp dưới đây để có thể mạnh mẽ hơn trên mạng.

- Tạo mật khẩu có tính bảo mật cao.
- Không dùng chung mật khẩu cho tất cả tài khoản.
- Đặt mật khẩu sáng tạo không ai đoán được.
- Tránh dùng thông tin cá nhân.
- Đừng ngại thay đổi mật khẩu.

HÃY THÔNG THÁI

Không gian mạng cũng có rất nhiều điểm tương đồng với cuộc sống thực tế của chúng ta. Những gì ta nói hoặc bày tỏ trên mạng thậm chí còn được nhiều người biết tới hơn và sự tồn tại của chúng là mãi mãi. Vậy phải làm sao để luôn là một người dùng thông thái trên mạng.

- Nhớ bảo vệ những bí mật cá nhân.
- Hãy thể hiện mặt tích cực của bản thân trên không gian mạng.
- Suy nghĩ kỹ trước khi đăng tải bất kỳ nội dung gì.

HÃY CẢNH GIÁC

Các chiêu thức lừa gạt trên mạng ngày càng nhiều và xuất hiện dày đặc hơn. Tuy nhiên, nếu chúng ta luôn học cách cảnh giác và bình tĩnh ứng phó khi gặp sự cố, mọi vấn đề sẽ có thể được phòng tránh và giải quyết ổn thỏa.

- Hãy kiểm tra lại tên miền của các trang web thật kỹ.
- Luôn sử dụng các web an toàn, không độc hại.
- Hãy cảnh giác với lừa đảo.

HÃY TỬ TẾ

- Hãy đối xử với người khác theo cách mà bạn muốn họ đối xử với bản thân mình. Lời khuyên này không chỉ rất đúng trong cuộc sống thực tế, mà còn có thể mang lại hiệu quả không nhỏ trên không gian mạng.
- Lan tỏa những điều tốt đẹp, chủ động lên tiếng để gỡ bỏ cái xấu, đó chắc chắn sẽ là những hành động đúng đắn để xây dựng một không gian mạng hạnh phúc và lành mạnh cho tất cả chúng ta.

HÃY DŨNG CẢM

Khi nhìn thấy các thông tin độc hại hoặc nhận được những nội dung không phù hợp từ người lạ, chúng ta thường dễ cảm thấy bối rối và chấp nhận bỏ qua rồi lờ đi những mẩu tin đó. Nhưng chúng ta có thể nói ra hoặc tìm cách báo cáo những điều độc hại đó, rất nhiều người khác sẽ tránh được nguy cơ bị đe dọa hoặc phải tiếp nhận nguồn tin xấu.

HÃY DŨNG CẢM

- Hãy lên tiếng.
- Chia sẽ cho người thân, cơ quan chức năng để nhận sự giúp đỡ.
- Ngăn chặn các nội dung không phù hợp.
- Lưu lại bằng chứng.
- Đừng sợ hãi.

CẢM ƠN QUÝ VỊ ĐÃ LẮNG NGHE !

FACEBOOK

https://www.facebook.com/Anninhmang.danang

ZALO

http://zalo.me/7347476256893694 49?src=qr

BAN QUẢN LÝ
KHU CÔNG NGHỆ CAO
VÀ CÁC KHU CÔNG NGHIỆP ĐÀ NẴNG

CÔNG AN THÀNH PHỐ ĐÀ NẴNG
PHÒNG AN NINH MẠNG VÀ PCTP
SỬ DỤNG CÔNG NGHỆ CAO

TẬP HUẤN

MỘT SỐ NỘI DUNG BẢO ĐẢM AN NINH MẠNG, BẢO VỆ BÍ MẬT NHÀ NƯỚC TRÊN KHÔNG GIAN MẠNG, BẢO VỆ DỮ LIỆU CÁ NHÂN

Thượng tá, Ths. **LÊ CAO TÂM**
Trưởng Phòng An ninh mạng
và PCTP sử dụng công nghệ cao

CÔNG AN TP ĐÀ NẴNG

PHÒNG AN NINH MẠNG VÀ PCTP SỬ DỤNG CÔNG NGHỆ CAO

Thượng úy Ngô Bá Toàn

SĐT liên hệ: 0903.623.678

Tài khoản Zalo "Bá Toàn"