LỚP TẬP HUẤN AN NINH MẠNG

Buổi 3 - Phòng chống mã độc và an toàn giao dịch trực tuyến

Mục tiêu của Buổi 3

- **Nhận biết** các loại phần mềm độc hại phổ biến và **cách phòng tránh** nhiễm độc.
- **Biết cách xử lý tình huống khẩn cấp** khi máy tính bị nhiễm virus.
- **Sử dụng mạng xã hội và thư điện tử công vụ** đúng quy chế an toàn.
- **Nắm vững các nguyên tắc giao dịch** thanh toán online an toàn.

Nội dung chính của Buổi 3

Phần 1 - Phòng chống phần mềm độc hại (Malware).

- Nhận biết các loại phần mềm độc hại phổ biến.
- Các biện pháp phòng tránh và bảo vệ hệ thống.

Phần 2 - An toàn giao dịch trực tuyến và sử dụng mạng xã hội.

- Nguyên tắc an toàn khi giao dịch trực tuyến.
- Sử dụng mạng xã hội an toàn, bảo vệ thông tin cá nhân.

Thực hành - Hướng dẫn thực hành Lab 3.

- Các bước thực hành theo hướng dẫn.
- Trải nghiệm và xử lý tình huống thực tế.

Tổng kết - Đánh giá và bế mạc khóa tập huấn.

- Đánh giá kết quả học tập.
- Tổng kết nội dung và giải đáp thắc mắc.

Phần 1 - Phòng chống phần mềm độc hại (Malware)

1. Khái niệm về các loại phần mềm độc hại.

Phần mềm được tạo ra với mục đích xấu, gây hại cho hệ thống,
đánh cắp dữ liệu hoặc làm gián đoạn hoạt động của máy tính.

2. Phân biệt Virus, Worm và Trojan.

Virus cần có file/host để lây lan, Worm tự nhân bản qua mạng,
Trojan ngụy trang thành phần mềm hợp pháp để đánh lừa người dùng.

3. Hiểm họa mã độc tống tiền Ransomware đối với cơ quan nhà nước.

Mã hóa dữ liệu, đòi tiền chuộc, gây gián đoạn dịch vụ công,
thiệt hại kinh tế và ảnh hưởng uy tín tổ chức.

4. Các con đường lây nhiễm mã độc chủ yếu.

Email độc hại, tệp đính kèm, USB, phần mềm bẻ khóa,
trang web độc hại, lỗ hổng phần mềm.

5. Quy trình ứng phó khẩn cấp khi máy tính bị nhiễm virus.

Ngắt kết nối mạng – Cô lập máy – Thông báo – Xử lý & diệt mã độc –
Khôi phục hệ thống – Thay đổi mật khẩu – Rút kinh nghiệm.

Khái niệm về mã độc (Malware)

Là **thuật ngữ chỉ chung** các loại phần mềm độc hại được kể xấu phát triển.

Nhằm **xâm nhập, phá hoại** hệ thống máy tính hoặc đánh cắp thông tin nhạy cảm.

Hoạt động ẩn danh, không có sự đồng ý của người sở hữu máy tính.

Gây ra các sự cố **mất an ninh mạng** nghiêm trọng cho cơ quan.

Virus máy tính - Cơ chế lây lan phá hoại

Là loại mã độc có khả năng **tự sao chép** và **đính kèm** vào các tệp tin sạch khác.

Cần sự **can thiệp của con người** để kích hoạt (ví dụ click mở file nhiễm virus).

Có thể **xóa dữ liệu**, làm hỏng hệ điều hành hoặc làm chậm máy tính.

Gây ra các sự cố **mất an ninh mạng** nghiêm trọng cho cơ quan.

Sâu máy tính (Worm)

– Nguy cơ tự lan truyền qua mạng nội bộ

1. Là loại mã độc **nâng cấp hơn virus**, có khả năng **tự động lấy lan**.

2. Không cần con người kích hoạt hay đính kèm vào file sạch.

3. Khai thác lỗ hổng mạng để tự động lây nhiễm từ máy này sang máy khác trong **mạng LAN** của cơ quan.

4. Có thể làm **nghẽn toàn bộ băng thông** mạng nội bộ chỉ trong thời gian ngắn.

Sâu máy tính có thể lây lan rất nhanh và khó kiểm soát, **gây gián đoạn nghiêm trọng đến hoạt động của hệ thống mạng nội bộ.**

Trojan (Mã độc gián điệp) - Cơ chế nguy trang tinh vi

1. **Ẩn mình dưới dạng** một phần mềm hữu ích, an toàn (ví dụ phần mềm đọc văn bản PDF, phần mềm gõ tiếng Việt).

2. **Khi người dùng cài đặt vào máy,** Trojan sẽ chạy ngầm bên dưới.

3. **Tiến hành ghi lại toàn bộ ký tự gõ từ bàn phím** (để cướp mật khẩu), chụp màn hình máy tính gửi về cho hacker.

QUY TRÌNH TẤN CÔNG

HẬU QUẢ

- Đánh cắp mật khẩu, tài khoản
- Lộ thông tin cá nhân và dữ liệu quan trọng
- Thiệt hại tài chính và uy tín

Mã độc quảng cáo (Adware) và Spyware theo đõi người dùng

ADWARE
(Mã độc quảng cáo)

Tự động hiển thị các cửa sổ quảng cáo trên màn hình, làm phiền người dùng và làm chậm máy tính.

SPYWARE
(Phần mềm gián điệp)

Thu thập lịch sử lướt web, địa chỉ IP và thông tin cá nhân của người dùng rồi gửi về máy chủ của kẻ quảng cáo hoặc tin tặc.

LƯU Ý

Cả Adware và Spyware đều ảnh hưởng đến hiệu suất và quyền riêng tư của người dùng.
Hãy luôn cài đặt phần mềm từ nguồn uy tín và sử dụng giải pháp bảo mật đáng tin cậy.

Cơ chế xâm nhập và mã hóa dữ liệu cơ quan của Ransomware

01

Thường xâm nhập qua tệp tin đính kèm **email giả mạo** hoặc lỗ hổng hệ điều hành chưa được vá lỗi.

02

Chạy ngầm để **quét toàn bộ ổ cứng** máy tính và các thư mục chia sẻ trong mạng LAN.

03

Thay đổi phần **đuôi mở rộng** của tệp tin thành đuôi lạ (ví dụ `.locked`).

04

Để lại file văn bản **thông báo đòi tiền chuộc** ngay trên màn hình nền.

Email giả mạo đính kèm tệp độc hại → Thực thi mã độc trên máy → Quét và mã hóa dữ liệu → Thay đổi đuôi tệp thành .locked → Hiển thị thông báo đòi tiền chuộc

Hậu quả nghiêm trọng khi hệ thống bị Ransomware tấn công

01

Toàn bộ hồ sơ công việc đang xử lý bị đóng băng

Làm gián đoạn dịch vụ công của cơ quan, ảnh hưởng đến hiệu suất và tiến độ công việc chung.

02

Gây tổn hại lớn đến uy tín chính trị của đơn vị

Ảnh hưởng nghiêm trọng đến niềm tin của người dân và đối tác vào năng lực quản lý, vận hành của cơ quan.

03

Chi phí khắc phuc, cải đặt lại hệ thống vô cùng tốn kém

Bao gồm chi phí khôi phục dữ liệu, nâng cấp hệ thống, thuê chuyên gia bảo mật và các chi phí phát sinh khác.

04

Nguy cơ lộ lọt dữ liệu cá nhân của người dân

Dữ liệu có thể bị rao bán hoặc sử dụng vào mục đích xấu, vi phạm quy định pháp luật về bảo vệ dữ liệu cá nhân.

CẢNH BÁO

Ransomware không chỉ là vấn đề kỹ thuật, mà còn là **mối đe dọa an ninh quốc gia**, ảnh hưởng trực tiếp đến hoạt động của cơ quan nhà nước và đời sống người dân.

Tại sao không nên trả tiền chuộc cho hacker?

01

Việc trả tiền chuộc không có bất kỳ sự đảm bảo nào là hacker sẽ gửi khóa giải mã.

Sau khi nhận tiền, hacker có thể biến mất hoặc không cung cấp khóa giải mã.

02

Nhiều trường hợp hacker nhận tiền xong rồi biến mất hoặc khóa dữ liệu lần thứ hai.

Hệ thống có thể bị tấn công lại hoặc dữ liệu bị bán cho nhóm hacker khác.

03

Trả tiền chuộc sẽ tạo tiền đề tài chính khuyến khích hacker tiếp tục tấn công các cơ quan khác.

Hành động này vô tình tiếp tay cho tội phạm mạng và làm gia tăng các cuộc tấn công.

04

Cách khắc phục duy nhất là phục hồi dữ liệu từ các bản sao lưu dự phòng an toàn trước đó.

Sao lưu định kỳ và kiểm tra bản sao lưu là biện pháp bảo vệ hiệu quả nhất.

HÃY BẢO VỆ DỮ LIỆU – ĐỪNG TIẾP TAY CHO TỘI PHẠM!

Đầu tư vào bảo mật và sao lưu dữ liệu định kỳ là giải pháp bền vững và an toàn nhất.

Các con đường lây nhiễm mã độc chủ yếu vào máy tính công sở

Mã độc không tự sinh ra trên máy tính mà lây nhiễm qua các thói quen sử dụng mạng chưa an toàn của người dùng.

Email lừa đảo và tệp đính kèm

Mở email từ địa chỉ không xác định, nhấp vào liên kết hoặc mở tệp đính kèm độc hại.

Tải xuống phần mềm không rõ nguồn gốc

Tải phần mềm từ trang web không uy tín, chứa cài đặt mã độc ẩn bên trong.

Thiết bị lưu trữ ngoài nhiễm độc

USB, ổ cứng di động bị nhiễm khi cắm vào máy tính mà không quét virus.

Truy cập website độc hại

Truy cập các trang web chứa mã độc khai thác lỗ hổng trình duyệt hoặc tự động tải về.

Lỗ hổng phần mềm chưa được vá

Phần mềm, hệ điều hành không cập nhật bản vá, kẻ xấu lợi dụng lỗ hổng để xâm nhập.

Hậu quả:

- Rò rỉ dữ liệu, mất thông tin quan trọng
- Hệ thống bị khóa, gián đoạn công việc
- Thiệt hại tài chính và uy tín của cơ quan
- Nguy cơ bị tấn công tiếp tục và lây lan rộng

LƯU Ý: Nâng cao nhận thức an toàn thông tin, tuân thủ quy định sử dụng và luôn cập nhật, vá lỗi là cách phòng tránh hiệu quả nhất.

Tải tệp tin lạ từ internet và cài đặt phần mềm không rõ nguồn gốc

1. Tải các phần mềm bẻ khóa hệ điều hành, phần mềm văn phòng lậu.

Các phần mềm này thường bị chèn mã độc, keylogger, ransomware...

2. Tải tệp tài liệu từ các trang web chia sẻ file miễn phí không uy tín.

File có thể bị chèn mã độc, virus hoặc chứa liên kết độc hại.

3. Bấm vào các quảng cáo trúng thưởng hoặc link tải phần mềm dọn dẹp máy tính giả mạo.

Đây là các chiêu trò lừa đảo, dẫn đến cài mã độc hoặc đánh cắp thông tin.

HẬU QUẢ:

- Nhiễm mã độc, ransomware.
- Bị đánh cắp dữ liệu, tài khoản.
- Thiệt hại tài chính và gián đoạn công việc.

Nhấp vào liên kết lạ trong email hoặc tin nhắn mạng xã hội

01

Bấm vào link rút gọn gửi từ tài khoản Zalo, Facebook của bạn bè bị hack.

Tin nhắn có link rút gọn có thể dẫn đến trang giả mạo để đánh cắp thông tin hoặc chiếm quyền tài khoản.

02

Mở tệp đính kèm trong Email công vụ từ người gửi lạ có tên file gây tò mò.

File đính kèm có thể chứa mã độc, virus hoặc chương trình gián điệp đánh cắp dữ liệu.

03

Quét các mã QR lạ dẫn đến các liên kết độc hại tại ứng dụng giả danh.

QR code có thể dẫn đến trang web giả mạo, yêu cầu cung cấp thông tin đăng nhập hoặc cài đặt ứng dụng độc hại.

KHUYẾN NGHỊ

- Không bấm vào link lạ, kể cả từ người quen.
- Không mở tệp đính kèm nếu không xác định rõ nguồn gốc.
- Không quét QR code từ nguồn không tin cậy.
- Luôn kiểm tra kỹ địa chỉ website trước khi cung cấp thông tin.

Sử dụng ổ đĩa USB đã bị nhiễm độc từ trước

01

Cắm USB dùng chung của cơ quan hoặc USB của khách hàng vào máy tính làm việc mà không thực hiện quét virus trước.

USB có thể chứa mã độc ẩn và lây nhiễm vào máy tính, đánh cắp dữ liệu hoặc phá hoại hệ thống.

02

Không tắt tính năng tự động chạy AutoPlay của USB trên máy tính.

AutoPlay có thể tự động mở và chạy file nguy hiểm khi cắm USB, gây rủi ro bảo mật cho hệ thống.

KHUYẾN NGHỊ

Quét virus trước khi sử dụng
Luôn quét virus cho USB bằng phần mềm diệt virus uy tín.

Tắt AutoPlay
Tắt tính năng AutoPlay để ngăn chặn nguy cơ tự động chạy mã độc.

Ưu tiên sử dụng USB an toàn
Chỉ sử dụng USB rõ nguồn gốc, được kiểm tra và tin cậy.

Thiết bị di động cá nhân kết nối vào mạng cơ quan

01

Điện thoại di động, máy tính bảng cá nhân đã bị nhiễm mã độc kết nối vào mạng Wi-Fi nội bộ của cơ quan.

Thiết bị nhiễm mã độc có thể mang mối đe dọa vào mạng nội bộ khi kết nối Wi-Fi.

02

Mã độc trên thiết bị cá nhân sẽ tìm cách dò quét lỗ hổng và tấn công sang máy tính làm việc của cán bộ cùng mạng.

Mã độc có thể khai thác lỗ hổng, đánh cắp dữ liệu, cài mã độc khác hoặc chiếm quyền điều khiển máy tính trong mạng nội bộ.

HẬU QUẢ

- Rò rỉ dữ liệu, thông tin nội bộ
- Lây lan mã độc trong mạng
- Chiếm quyền hệ thống, dữ liệu
- Gián đoạn hoạt động của cơ quan

KHUYẾN NGHỊ AN TOÀN

Hạn chế kết nối
Hạn chế hoặc không cho phép thiết bị cá nhân kết nối vào Wi-Fi nội bộ cơ quan.

Kiểm tra bảo mật
Cài đặt và cập nhật phần mềm chống virus trên thiết bị cá nhân thường xuyên.

Cập nhật hệ thống
Luôn cập nhật hệ điều hành và ứng dụng để vá các lỗ hổng bảo mật.

Tuân thủ quy định
Tuân thủ quy định của cơ quan về việc sử dụng thiết bị cá nhân và truy cập mạng.

Biện pháp phòng chống mã độc bằng phần mềm Antivirus

01

Sử dụng phần mềm diệt virus là lá chắn bắt buộc đối với máy tính công sở:

Cài đặt và luôn bật phần mềm Antivirus được cấp phép để bảo vệ thiết bị và dữ liệu của cơ quan.

02

Quét thời gian thực (Real-time protection) - Chế độ bảo vệ luôn chạy ngầm

để phát hiện và ngăn chặn mã độc ngay khi chúng vừa tải về hoặc thực thi.

03

Quét định kỳ (Scheduled scan) - Cấu hình quét toàn bộ ổ cứng hàng tuần

để phát hiện mã độc ẩn sâu trong hệ thống.

04

Cập nhật dữ liệu thường xuyên - Đảm bảo phần mềm diệt virus luôn được cập nhật

mẫu nhận diện mới nhất từ nhà sản xuất để đối phó với virus mới.

LƯU Ý: | Luôn bật phần mềm Antivirus | Không tắt các tính năng bảo vệ | Thực hiện quét định kỳ | Cập nhật thường xuyên

Sử dụng Windows Defender Antivirus trên Windows 10/11

- **Công cụ tích hợp sẵn -** Windows Defender là phần mềm diệt virus miễn phí, chất lượng cao đi kèm hệ điều hành Windows.
- **Bật tính năng bảo vệ -** Luôn đảm bảo mục Real-time protection và Cloud-delivered protection được bật trong cài đặt bảo mật (Windows Security).
- **Cách quét thủ công -** Người dùng có thể nhấp chuột phải vào bất kỳ tệp tin/thư mục nào và chọn Scan with Microsoft Defender để kiểm tra nhanh.

Miễn phí & tích hợp
Có sẵn trên Windows 10/11, không cần cài đặt thêm.

Bảo vệ thời gian thực
Phát hiện và ngăn chặn mã độc ngay khi tải về hoặc thực thi.

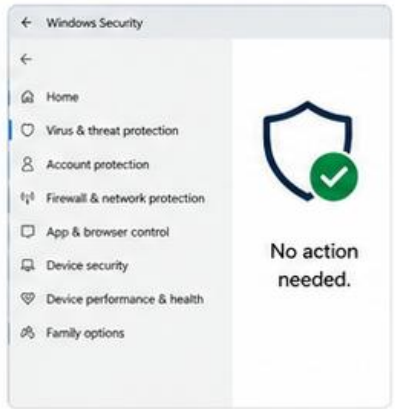
Bảo vệ đám mây
Cloud-delivered protection giúp nhận diện mối đe dọa mới nhất.

Quét linh hoạt
Quét nhanh, quét toàn bộ hoặc quét tùy chọn theo nhu cầu.

HƯỚNG DẪN THỰC HIỆN

1 Mở Windows Security

- Nhấn Start → gõ "Windows Security" và mở ứng dụng.

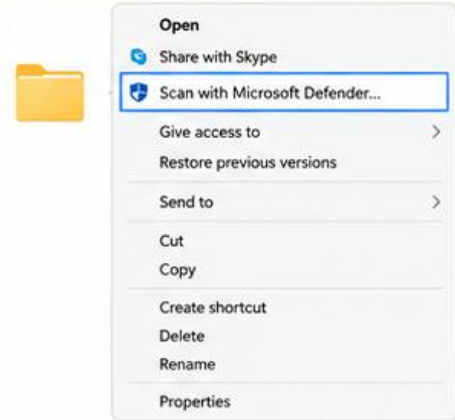


2 Kiểm tra cài đặt bảo vệ

- Chọn "Virus & threat protection"
- Đảm bảo bật:
  - Real-time protection
  - Cloud-delivered protection

3 Quét thủ công với Microsoft Defender

- Nhấp chuột phải vào tệp tin hoặc thư mục cần quét.
- Chọn "Scan with Microsoft Defender".



LƯU Ý QUAN TRỌNG

- Luôn cập nhật Windows để nhận bản vá bảo mật mới nhất.
- Không tắt Real-time protection trừ khi có lý do đặc biệt.
- Thường xuyên quét hệ thống để phát hiện mối đe dọa ẩn.
- Cập nhật Windows Defender để có cơ sở dữ liệu mới nhất.

Quy trình ứng phó khẩn cấp khi nghi ngờ máy tính nhiễm virus

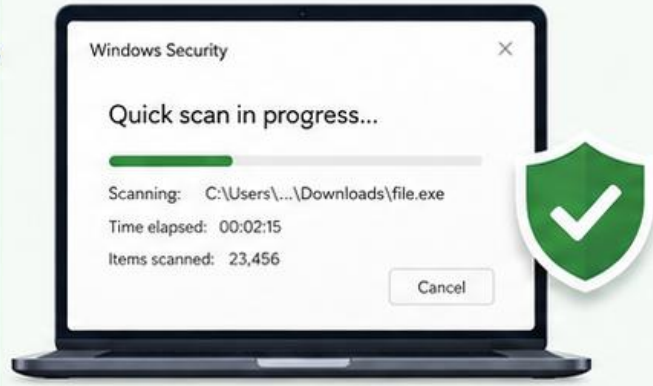
Khi máy tính xuất hiện dấu hiệu lạ như tự động mở trang web lạ, file văn bản bị đổi đuôi hoặc máy chạy cực kỳ chậm, người dùng cần lập tức thực hiện 3 bước sau.

01 NGẮT KẾT NỐI

Ngắt kết nối Internet (Wi-Fi / dây mạng) và các thiết bị ngoại vi (USB, ổ cứng ngoài,...) để ngăn virus lây lan.

02 KIỂM TRA VÀ XỬ LÝ

Dùng phần mềm diệt virus (như Windows Defender) quét toàn bộ hệ thống để phát hiện và xử lý mã độc.



03 KHÔI PHỤC VÀ PHÒNG NGỪA

Khôi phục dữ liệu an toàn (nếu có bản sao lưu), cập nhật hệ điều hành và phần mềm, đồng thời đổi mật khẩu các tài khoản quan trọng.

LƯU Ý QUAN TRỌNG

- Không tiếp tục sử dụng máy tính khi nghi ngờ nhiễm virus.
- Không tắt phần mềm diệt virus hoặc bỏ qua cảnh báo.
- Sao lưu dữ liệu thường xuyên để hạn chế thiệt hại.
- Nếu không tự xử lý được, hãy liên hệ bộ phận IT để được hỗ trợ.

BƯỚC 1 - NGẮT KẾT NỐI MẠNG NGAY LẬP TỨC

01

Rút cáp mạng LAN

Rút ngay lập tức cáp mạng LAN đang được cắm ở phía sau thùng máy tính để bàn (PC) của bạn.

02

Tắt kết nối Wi-Fi

Ngắt kết nối mạng không dây (Wi-Fi) hoặc chuyển sang chế độ máy bay nếu bạn đang sử dụng máy tính xách tay.

Việc này giúp **cô lập hoàn toàn** máy tính bị nhiễm, ngăn chặn mã độc/virus tiếp tục lây

BƯỚC 2 - GIỮ NGUYÊN HIỆN TRẠNG MÁY TÍNH

Tuyệt đối KHÔNG tiếp tục nhập mật khẩu

Ngừng ngay việc đăng nhập tài khoản công vụ, email, hoặc mật khẩu ngân hàng trên máy tính đang bị nghi ngờ nhiễm virus để tránh **bị đánh cắp thông tin**.

KHÔNG tự ý cài đặt thêm phần mềm

Không tải xuống hoặc cài đặt các phần mềm diệt virus, công cụ sửa lỗi lạ từ internet. Việc này có thể tải thêm **mã độc giả mạo** vào hệ thống.

KHÔNG tắt nguồn đột ngột (rút điện)

Nếu không thật sự cần thiết, đừng rút phích cắm. Việc tắt máy đột ngột có thể làm mất các **dữ liệu tạm thời (RAM)** rất quan trọng để bộ phận IT phân tích mã độc.

Việc giữ nguyên hiện trạng giúp **bảo vệ dữ liệu nhạy cảm** của bạn và tạo điều kiện tốt nhất để đội ngũ kỹ thuật **truy vết và xử lý triệt để** sự cố.

BƯỚC 3 - BÁO CÁO SỰ CỐ KỊP THỜI

1

Liên hệ ngay bộ phận CNTT

Thông báo ngay lập tức cho **cán bộ phụ trách CNTT** hoặc ban an ninh mạng của đơn vị để họ có mặt và hỗ trợ chuyên môn.

2

Cung cấp chi tiết sự cố

Nhớ lại và thông báo chính xác về **tệp tin lạ vừa mở** hoặc **đường link vừa click** ngay trước khi máy tính xuất hiện dấu hiệu bất thường.

3

Tuân thủ tuyệt đối hướng dẫn

Không tự ý hành động. Hãy **nghiêm túc thực hiện** mọi yêu cầu và hướng dẫn xử lý tiếp theo từ cán bộ kỹ thuật chuyên trách.

Sự **minh bạch và phối hợp chặt chẽ** của bạn với bộ phận CNTT là yếu tố quyết định để khống chế sự cố nhanh chóng và giảm thiểu tối đa thiệt hại cho tổ chức.

NỘI DUNG CHÍNH

An toàn giao dịch trực tuyến và sử dụng mạng xã hội

01

Mạng Xã Hội

Nắm vững các **nguyên tắc an toàn** khi sử dụng các nền tảng phổ biến như Zalo, Facebook.

02

Bảo Mật 2 Lớp

Cách thiết lập **xác thực hai lớp (2FA)** để bảo vệ tài khoản khỏi nguy cơ bị xâm nhập.

03

Email Công Vụ

Tuân thủ nghiêm ngặt các **quy chế sử dụng** Hệ thống Thư điện tử công vụ.

04

Thanh Toán

Các nguyên tắc cốt lõi đảm bảo an toàn khi thanh toán trực tuyến qua **Smart Banking**.

NGUYÊN TẮC TRỌNG TÂM

SỬ DỤNG MẠNG XÃ HỘI CHUẨN MỰC

01

Nhận diện rủi ro

Mạng xã hội (Zalo, Facebook) giúp kết nối công việc nhanh chóng nhưng luôn tiềm ẩn **nhiều rủi ro bảo mật thông tin**.

02

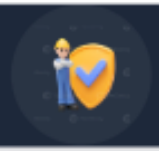
Phân định tài khoản

Cán bộ cần **tách bạch rõ ràng** giữa tài khoản phục vụ công việc chuyên môn và tài khoản cá nhân dành cho giải trí.

03

Tuân thủ quy định

Nghiêm túc thực hiện **Quy tắc ứng xử trên mạng xã hội** của cán bộ, công chức, viên chức do nhà nước ban hành.



TINH THẦN TRÁCH NHIỆM

Sử dụng mạng xã hội có ý thức và đúng mục đích không chỉ bảo vệ an toàn thông tin mà còn **giữ gìn uy tín, hình ảnh chuyên nghiệp** của cơ quan.

CẢNH BÁO AN TOÀN

Nguy cơ rò rỉ tài liệu & thông tin cá nhân

01

Đăng tải văn bản nội bộ

Tuyệt đối không tự ý chụp ảnh và đăng tải các văn bản dự thảo, quyết định nội bộ của cơ quan lên trang mạng xã hội cá nhân.

02

Nhóm chat thiếu bảo mật

Tránh trao đổi thông tin nghiệp vụ mật qua các nhóm chat công cộng vì chúng thường không được mã hóa đầu cuối an toàn.

03

Lộ lọt thông tin cá nhân

Việc chia sẻ hình ảnh thẻ công chức, căn cước sẽ tạo điều kiện cho tin tặc thu thập dữ liệu phục vụ mục đích lừa đảo giả danh.

NGUYÊN TẮC BẢO MẬT

Sự bất cẩn nhỏ trên mạng xã hội có thể dẫn đến hậu quả nghiêm trọng cho tổ chức. Hãy luôn kiểm tra kỹ lưỡng thông tin trước khi nhấn nút "Chia sẻ".

AN TOÀN MẠNG XÃ HỘI

Hướng dẫn thiết lập bảo mật tài khoản Facebook

01

Mật khẩu mạnh & duy nhất

Thiết lập mật khẩu có độ khó cao, kết hợp chữ, số và ký tự đặc biệt. **Tuyệt đối không dùng chung mật khẩu** với tài khoản khác.

02

Cảnh báo đăng nhập lạ

Kích hoạt tính năng thông báo bảo mật để nhận ngay cảnh báo khi có **thiết bị hoặc vị trí mới** cố gắng truy cập tài khoản.

03

Kiểm soát quyền riêng tư

Cấu hình lại cài đặt để giới hạn danh sách bạn bè và thông tin liên hệ cá nhân (SĐT, Email) ở chế độ **"Chỉ bạn bè"** (Friends only).

NGUYÊN TẮC PHÒNG VỆ

Bảo mật tài khoản cá nhân an toàn chính là xây dựng **lớp phòng tuyến đầu tiên** ngăn chặn kẻ xấu xâm nhập và đánh cắp thông tin nhạy cảm của tổ chức.

AN TOÀN TIN NHẮN

Thiết lập bảo mật tài khoản Zalo công việc

01

Khóa Ứng Dụng

Sử dụng tính năng Khóa Zalo bằng **mã PIN 4 số** trên thiết bị di động để bảo vệ nội dung tin nhắn.

02

Ẩn Số Điện Thoại

Tắt tính năng tự động hiển thị số điện thoại cá nhân đối với **người lạ** để bảo vệ thông tin liên lạc.

03

Chặn Tìm Kiếm

Vô hiệu hóa tính năng cho phép người lạ **tìm kiếm tài khoản** thông qua số điện thoại của bạn.

04

Quản Lý Thiết Bị

Thường xuyên kiểm tra danh sách thiết bị truy cập và lập tức **đăng xuất** khỏi các thiết bị lạ.

NGUYÊN TẮC BẢO MẬT

Kiểm soát chặt chẽ quyền riêng tư trên Zalo là **lớp lá chắn quan trọng** ngăn chặn kẻ gian thu thập thông tin và tiếp cận hệ thống nội bộ.

ỨNG DỤNG NHẮN TIN OTT

An toàn khi sử dụng Viber & Telegram

Rủi ro tiềm ẩn trên ứng dụng nhắn tin

Telegram và Viber được sử dụng phổ biến trong trao đổi công việc nhờ tính năng đa dạng, tuy nhiên, chúng cũng **tiềm ẩn nhiều nguy cơ cao** về bảo mật nếu không được thiết lập đúng cách.

Tắt "Tự động tải xuống" (Auto-download)

Ngăn chặn nguy cơ thiết bị tự động lưu các file phương tiện chứa **mã độc ẩn** từ các nguồn không xác định.

Cảnh giác với các nhóm lạ ẩn danh

Thiết lập quyền riêng tư để chặn tính năng tự động bị thêm vào các nhóm chat quảng cáo, **bẫy lừa đảo tài chính** giả mạo.

Sử dụng tính năng Mã hóa đầu cuối

Bắt buộc kích hoạt tính năng **Trò chuyện bí mật (Secret Chat)** để chống nghe lén khi trao đổi thông tin nghiệp vụ nhạy cảm.

Chủ động thiết lập quyền riêng tư chặt chẽ ngay từ đầu là cách tốt nhất để bảo vệ dữ liệu nội bộ trên các ứng dụng nhắn tin OTT.

CẤU HÌNH HỆ THỐNG

Biện pháp thiết lập an toàn trên Telegram & Viber

Tắt tải tệp tin tự động

Ngăn chặn nguy cơ nhiễm mã độc ẩn trong các file phương tiện tải về ngoài ý muốn.

> Settings > Data and Storage > Tắt **Automatic media download**

Chặn thêm vào nhóm lạ

Tránh bị lôi kéo vào các hội nhóm lừa đảo ẩn danh, giả mạo đầu tư tài chính.

> Settings > Privacy and Security > Groups & Channels > Đổi sang **My Contacts**

Xác thực hai bước (2FA)

Tạo thêm một lớp bảo vệ vững chắc khi đăng nhập tài khoản trên các thiết bị mới.

> Settings > Privacy and Security > Bật **Two-Step Verification**

Ẩn số điện thoại cá nhân

Tránh bị thu thập dữ liệu cá nhân phục vụ cho các chiến dịch gọi điện, nhắn tin lừa đảo.

> Settings > Privacy and Security > Phone Number > Chọn **Nobody**

NGUYÊN TẮC QUAN TRỌNG

Mặc định của ứng dụng thường hướng tới sự tiện lợi. Chủ động **thiết lập lại quyền riêng tư** là bước bắt buộc để bảo vệ dữ liệu nội bộ an toàn.

An toàn khi sử dụng các dịch vụ điện toán đám mây

Google Drive, OneDrive, iCloud mang lại sự thuận tiện nhưng tiềm ẩn rủi ro nếu cấu hình sai.

Chia sẻ công khai không kiểm soát

Thói quen để quyền truy cập **"Anyone with the link"** (Bất kỳ ai có liên kết) khiến tài liệu nội bộ dễ dàng bị rò rỉ và phát tán không thể thu hồi.

Lưu trữ dữ liệu mật chưa mã hóa

Tuyệt đối không đưa các tài liệu mật, tệp chứa mật khẩu, hoặc thông tin cá nhân dưới dạng **file thô** (chưa mã hóa) lên đám mây công cộng.

Nguy cơ đồng bộ tự động mã độc

Nếu máy tính nhiễm virus, các **file nhiễm độc sẽ tự động đồng bộ** lên đám mây, từ đó lây lan sang các máy tính khác cùng sử dụng dịch vụ.

Đám mây là nơi lưu trữ, không phải két sắt an tuyệt đối. Hãy phân quyền chặt chẽ và mã hóa dữ liệu!

Hướng dẫn chia sẻ dữ liệu an toàn trên đám mây

Đảm bảo an toàn cho tài liệu nội bộ bằng cách tuân thủ 4 nguyên tắc phân quyền sau.

01

Hạn chế đối tượng

Chỉ chia sẻ đích danh qua địa chỉ email của người nhận (quyền **Restricted**). Tuyệt đối không sử dụng liên kết chia sẻ công khai.

02

Chọn đúng phân quyền

Ưu tiên thiết lập quyền **Viewer** (Chỉ xem) hoặc **Commenter** (Nhận xét). Hạn chế tối đa việc cấp quyền Editor (Người chỉnh sửa).

03

Khóa tải & sao chép

Với các tài liệu nội bộ quan trọng, hãy bật tính năng **ngăn chặn người xem tải xuống**, in ấn hoặc sao chép nội dung tệp tin.

04

Đặt thời hạn liên kết

Chủ động thiết lập **thời gian hết hạn** cho liên kết chia sẻ (nếu nền tảng hỗ trợ) để hệ thống tự động thu hồi quyền truy cập.

Chia sẻ đúng người, cấp đúng quyền và giới hạn thời gian để bảo vệ tài liệu tổ chức!

Khái niệm Xác thực hai lớp (2FA) và sự cần thiết của nó

- Là phương pháp xác minh danh tính người dùng bằng cách yêu cầu cung cấp 2 yếu tố chứng thực khác nhau.

- Giúp bảo vệ tài khoản an toàn ngay cả khi hacker đã biết được mật khẩu đăng nhập của người dùng.

- Là chốt chặn bảo mật bắt buộc đối với tất cả các tài khoản trực tuyến quan trọng.

Cách hoạt động của 2FA bảo vệ tài khoản của bạn

- **Yếu tố 1** - Mật khẩu đăng nhập thông thường của người dùng (những gì người dùng biết).
- **Yếu tố 2** - Mã OTP gửi về tin nhắn SMS điện thoại hoặc mã số ngẫu nhiên sinh ra trên ứng dụng Google Authenticator (những gì người dùng có).
- Hacker ở xa chỉ có mật khẩu của người dùng cũng không thể đăng nhập được vì thiếu điện thoại cá nhân của người dùng để nhận mã OTP.

Quy chế sử dụng Hệ thống Thư điện tử công vụ đúng quy định

- Thư điện tử công vụ (đuôi `.gov.vn`) được cấp riêng phục vụ hoạt động chuyên môn hành chính.

- Bắt buộc phải sử dụng **email công vụ** khi gửi nhận văn bản, tài liệu công việc của cơ quan.

- Không sử dụng các hộp thư miễn phí như **Yahoo, Gmail** để trao đổi công văn nội bộ của đơn vị.

Những hành vi bị cấm khi sử dụng email công vụ

- **Tuyệt đối không** dùng email công vụ để đăng ký tài khoản mạng xã hội cá nhân (Facebook, Tiktok).

- **Không dùng** email công vụ để đăng ký tài khoản mua sắm trực tuyến (Shopee, Lazada) hoặc diễn đàn giải trí.

- **Không gửi** thư điện tử chứa nội dung xúc phạm, quảng cáo thương mại hoặc phát tán thông tin sai lệch từ hộp thư công vụ.

Nguy cơ mất an toàn khi chuyển tiếp tự động thư công vụ sang email cá nhân

- Tính năng **tự động chuyển tiếp (auto-forward)** thư điện tử công vụ sang Gmail cá nhân tiềm ẩn rủi ro lộ lọt dữ liệu rất lớn.

- Hòm thư Gmail cá nhân thường **không được cấu hình bảo mật nghiêm ngặt** và **dễ bị hack.**

- Việc chuyển tiếp dữ liệu nội bộ ra máy chủ bên ngoài **vi phạm quy chế an ninh mạng** của cơ quan nhà nước.

Hãy **tắt tính năng tự động chuyển tiếp** và chỉ truy cập thư công vụ trên hệ thống chính thống để bảo vệ thông tin của cơ quan và của bạn.

An toàn giao dịch ngân hàng số (Smart Banking)

- Giao dịch thanh toán trực tuyến mang lại nhiều tiện ích nhưng là mục tiêu hàng đầu của tội phạm tài chính.

- Cần tuân thủ các quy tắc bảo mật nghiêm ngặt khi thực hiện chuyển tiền qua ứng dụng di động.

Cảnh giác cuộc gọi giả danh nhân viên ngân hàng hoặc công an yêu cầu cung cấp OTP

01 Đối tượng gọi điện thông báo người dùng có khoản nợ thẻ tín dụng hoặc tài khoản bị xâm nhập.

02 Yêu cầu người dùng quét mã QR hoặc đăng nhập vào link giả mạo ngân hàng để nhập OTP xác minh.

03 Khi người dùng nhập OTP vào trang web giả mạo, kẻ xấu sẽ lập tức rút hết tiền trong tài khoản của người dùng.

CẢNH GIÁC VỚI MÃ QR LẠ TRÊN MẠNG XÃ HỘI

01 Kẻ xấu gửi mã QR lạ qua Zalo nhờ người dùng quét để nhận tiên hỗ trợ hoặc xem tài liệu.

02 Quét mã QR thực chất là thao tác điều hướng trình duyệt đến một trang web lừa đảo lấy mật khẩu hoặc tài mã độc vê điện thoại.

03 Chỉ quét mã QR khi biết rõ nguồn gốc và nội dung trang web đích.

Sử dụng sinh trắc học để nâng cao độ bảo mật

01 Kích hoạt tính năng **xác thực sinh trắc học** (vân tay, nhận diện khuôn mặt FaceID) trên ứng dụng Smart Banking.

02 Giúp đăng nhập và xác thực chuyển tiền **nhanh chóng** mà không lo bị người bên cạnh nhìn trộm mã PIN.

03 Theo quy định mới, các giao dịch chuyển tiền có giá trị lớn bắt buộc phải **xác thực sinh trắc học** để phòng ngừa lừa đảo chiếm đoạt tài khoản.

LƯU Ý: Hãy cập nhật ứng dụng Smart Banking lên phiên bản mới nhất để trải nghiệm đầy đủ tính năng và bảo mật tối ưu.

BẢO MẬT TUYỆT ĐỐI | GIAO DỊCH NHANH CHÓNG | AN TÂM MỌI LÚC

CẢM ƠN VÀ THẢO LUẬN BUỔI 3