LỚP TẬP HUẤN AN NINH MẠNG

BUỔI 2 - BẢO MẬT THIẾT BỊ, KẾT NỐI AN TOÀN VÀ SAO LƯU DỮ LIỆU

MỤC TIÊU CỦA BUỔI 2

- LÀM CHỦ CÁC TÍNH NĂNG BẢO MẬT TÍCH HỢP TRÊN HỆ ĐIỀU HÀNH WINDOWS.
- BIẾT CÁCH PHÒNG NGỪA MÃ ĐỘC LÂY TRUYỀN QUA THIẾT BỊ NGOẠI VI USB.
- THỰC HÀNH KẾT NỐI MẠNG CÔNG CỘNG AN TOÀN, TRÁNH BỊ NGHE LÉN THÔNG TIN.
- NẮM RÕ QUY TRÌNH PHÂN LOẠI DỮ LIỆU, NÉN MÃ HÓA VÀ SAO LƯU TÀI LIỆU.

NỘI DUNG CHÍNH CỦA BUỔI 2

PHẦN 1 - Bảo mật thiết bị và hệ điều hành Windows.

PHẦN 2 - Nguyên tắc kết nối an toàn với USB và Wi-Fi công cộng.

PHẦN 3 - Quy trình phân loại, mã hóa và sao lưu dữ liệu văn phòng.

THỰC HÀNH - Hướng dẫn thực hành Lab 2.

PHẦN 1 - BẢO MẬT THIẾT BỊ VÀ HỆ ĐIỀU HÀNH WINDOWS

- TẦM QUAN TRỌNG CỦA VIỆC BẢO VỆ HỆ ĐIỀU HÀNH LÀM VIỆC HẰNG NGÀY.
- QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG TRÊN MÁY TÍNH WINDOWS.
- THIẾT LẬP TƯỜNG LỬA BẢO VỆ MÁY TÍNH TRƯỚC CÁC KẾT NỐI LẠ.
- QUY TRÌNH CẬP NHẬT BẢN VÁ LỖI CHO HỆ THỐNG.

TẦM QUAN TRỌNG CỦA AN TOÀN HỆ ĐIỀU HÀNH

MÁY TÍNH VĂN PHÒNG

Là nơi xử lý và lưu trữ phần lớn hồ sơ, văn bản hành chính.

HỆ ĐIỀU HÀNH WINDOWS

Là mục tiêu tấn công hàng đầu của tin tặc.

MỘT SƠ HỞ NHỎ TRONG CẤU HÌNH

Windows có thể dẫn đến việc lộ lọt dữ liệu cơ quan.

QUẢN LÝ TÀI KHOẢN NGƯỜI DÙNG TRÊN WINDOWS

Hệ điều hành Windows chia tài khoản sử dụng thành các cấp độ phân quyền khác nhau:

01

TÀI KHOẢN QUẢN TRỊ (ADMINISTRATOR)

Có toàn quyền kiểm soát hệ thống.
Có thể cài đặt phần mềm, thay đổi cấu hình và quản lý tất cả tài khoản người dùng.

02

TÀI KHOẢN NGƯỜI DÙNG TIÊU CHUẨN (STANDARD USER)

Có thể sử dụng các ứng dụng và thay đổi cài đặt cá nhân, nhưng không được phép thay đổi hệ thống.

03

TÀI KHOẢN KHÁCH (GUEST)

Có quyền hạn chế, dùng tạm thời.
Không thể thay đổi hệ thống và dữ liệu của người khác.

LƯU Ý

- Không nhập thông tin cá nhân, tài khoản, mật khẩu vào các trang web không rõ nguồn gốc.
- Khi nghi ngờ, hãy truy cập trực tiếp trang web chính thức bằng cách gõ tên miền vào trình duyệt.
- Liên hệ với cơ quan, tổ chức qua kênh chính thức để xác minh thông tin.

SO SÁNH TÀI KHOẢN ADMINISTRATOR VÀ STANDARD USER

TIÊU CHÍ	TÀI KHOẢN ADMINISTRATOR	TÀI KHOẢN STANDARD USER
QUYỀN HẠN	Có toàn quyền kiểm soát hệ thống, bao gồm cài đặt, thay đổi và quản lý tất cả chức năng.	Chỉ có quyền hạn cơ bản để sử dụng hệ thống, không can thiệp vào các thiết lập quan trọng.
CÀI ĐẶT PHẦN MỀM	Có thể cài đặt, gỡ bỏ bất kỳ phần mềm nào trên hệ thống.	Chỉ được cài đặt các ứng dụng sẵn có hoặc được quản trị viên cho phép.
THAY ĐỔI HỆ THỐNG	Có thể thay đổi các cấu hình hệ thống, cài đặt mạng, tài khoản người dùng, cập nhật hệ thống,...	Không được phép thay đổi các cấu hình hệ thống hoặc cài đặt quan trọng.
TRUY CẬP TÀI LIỆU KHÁC	Có thể truy cập, đọc, sửa, xóa dữ liệu của người dùng khác (nếu được cấp quyền).	Chỉ truy cập và quản lý dữ liệu trong phạm vi tài khoản của mình.
MỨC ĐỘ AN TOÀN	Nếu bị xâm nhập, rủi ro cao vì có thể bị kiểm soát toàn bộ hệ thống.	An toàn hơn, hạn chế rủi ro do không thể thay đổi các thiết lập quan trọng của hệ thống.

KẾT LUẬN

Nên sử dụng tài khoản Standard User cho công việc hàng ngày.
Chỉ sử dụng tài khoản Administrator khi cần cài đặt phần mềm hoặc thay đổi cấu hình hệ thống.

NGUY CƠ ĐĂNG NHẬP HẰNG NGÀY BẰNG TÀI KHOẢN QUẢN TRỊ ADMIN

Sử dụng tài khoản Admin hàng ngày tiềm ẩn nhiều rủi ro ảnh hưởng đến an toàn hệ thống và dữ liệu.

01

RỦI RO QUYỀN CAO

Nếu người dùng dùng tài khoản Admin làm việc hàng ngày, khi vô tình tải file chứa mã độc, mã độc sẽ tự chạy với quyền Admin cao nhất.

02

DỄ BỊ TẤN CÔNG

Nó sẽ tự cài đặt vào hệ thống, tắt phần mềm diệt virus và mã hóa dữ liệu.

03

KHUYÊN NGHỊ

Sử dụng tài khoản người dùng tiêu chuẩn cho công việc hàng ngày.

KHUYÊN NGHỊ

Chỉ sử dụng tài khoản Admin khi cần cài đặt phần mềm, thay đổi cấu hình hệ thống hoặc thực hiện các tác vụ quản trị quan trọng.

Thiết lập mật khẩu đăng nhập máy tính công sở

01

YÊU CẦU BẮT BUỘC

Máy tính làm việc tại cơ quan bắt buộc phải cài đặt mật khẩu đăng nhập mạnh.

02

ÁP DỤNG QUY TẮC

Mật khẩu đăng nhập Windows nên áp dụng quy tắc cụm từ mật mã.

03

TRÁNH MẬT KHẨU YẾU

Tuyệt đối không để trống mật khẩu hoặc đặt mật khẩu quá đơn giản như `123456`.

LƯU Ý: Sử dụng mật khẩu mạnh giúp bảo vệ dữ liệu, hạn chế rủi ro xâm nhập và đảm bảo an toàn thông tin của cơ quan.

TÍNH NĂNG TỰ ĐỘNG KHÓA MÀN HÌNH KHI KHÔNG LÀM VIỆC

01 **Khi rời bàn làm việc để đi họp hoặc giải lao,** người dùng có thói quen để máy tính mở.

02 Đây là cơ hội để người lạ tiếp cận và sao chép dữ liệu trên máy tính.

03 Cần cài đặt thời gian tự động khóa màn hình sau **3 đến 5 phút** không hoạt động.

04 Người dùng nên nhấn phím tắt **Windows + L** để khóa máy ngay lập tức khi rời đi.

LỢI ÍCH | Giúp bảo vệ thông tin cá nhân và dữ liệu quan trọng, hạn chế rủi ro bị truy cập trái phép.

KHÁI NIỆM VỀ TƯỜNG LỬA CÁ NHÂN (FIREWALL)

01

RÀO CHẮN KIỂM SOÁT

Là một rào chắn kiểm soát lưu lượng mạng ra vào máy tính.

02

NGĂN CHẶN TRÁI PHÉP

Ngăn chặn các nỗ lực truy cập trái phép từ các máy tính khác trong mạng nội bộ.

03

TÍCH HỢP SẴN

Được tích hợp sẵn trên Windows dưới tên gọi Windows Defender Firewall.

LỢI ÍCH

- Bảo vệ dữ liệu cá nhân và thông tin quan trọng.
- Giúp hệ thống an toàn hơn khi kết nối mạng.
- Giảm thiểu nguy cơ bị tấn công từ phần mềm độc hại.

Cơ chế hoạt động bảo vệ của Windows Defender Firewall

Lọc và kiểm soát lưu lượng mạng để bảo vệ máy tính của bạn

01

GIÁM SÁT KẾT NỐI MẠNG

Giám sát các cổng kết nối mạng của máy tính.

02

CHẶN KẾT NỐI TRÁI PHÉP

Chặn tất cả các kết nối từ bên ngoài vào máy tính trừ các kết nối đã được cho phép.

03

PHÁT HIỆN VÀ CẢNH BÁO

Phát hiện và cảnh báo khi một ứng dụng trên máy cố gắng gửi dữ liệu ra ngoài Internet.

LƯU Ý: Windows Defender Firewall hoạt động âm thầm trong nền, đảm bảo an toàn mạng mà không làm gián đoạn công việc của bạn.

HƯỚNG DẪN CẤU HÌNH TƯỜNG LỬA LUÔN HOẠT ĐỘNG AN TOÀN

01

Truy cập vào mục **Windows Defender Firewall** trong **Control Panel** hoặc **Settings**.

02

Đảm bảo trạng thái tường lửa luôn ở chế độ bật (Turn on **Windows Defender Firewall**).

03

Không tự ý bấm đồng ý tắt tường lửa khi nhận được yêu cầu từ các phần mềm lạ.

LƯU Ý

- Tường lửa giúp bảo vệ thiết bị của bạn khỏi các kết nối không an toàn.
  Chỉ tắt tường lửa khi có hướng dẫn rõ ràng từ chuyên gia hoặc khi thật sự cần thiết.

Khải nghiệm bản và bảo mật hệ thống

01

Hệ điều hành Windows chứa hàng triệu dòng mã và không tránh khỏi các lỗi lập trình.

02

Hacker khai thác các lỗi này (gọi là lỗ hổng bảo mật) để xâm nhập máy tính.

03

Microsoft

Nhà sản xuất Microsoft liên tục phát hành các bản sửa lỗi, gọi là bản vá bảo mật.

LƯU Ý

Luôn cập nhật hệ điều hành và phần mềm để vá các lỗ hổng và bảo vệ hệ thống của bạn an toàn hơn.

TẦM QUAN TRỌNG CỦA CẬP NHẬT WINDOWS UPDATE THƯỜNG XUYÊN

01

GIÚP MÁY TÍNH VÀ CÁC LỖ HỔNG BẢO MẬT MỚI NHẤT

Giúp máy tính và các lỗ hổng bảo mật mới nhất để phòng ngừa tin tặc khai thác.

02

CẢI THIỆN TÍNH ỔN ĐỊNH VÀ HIỆU NĂNG

Cải thiện tính ổn định và hiệu năng làm việc của máy tính.

03

GIÚP HỆ THỐNG PHÁT HIỆN TỐT HƠN MÃ ĐỘC, PHẦN MỀM ĐỘC HẠI MỚI

Giúp hệ thống phát hiện tốt hơn các mối virus, phần mềm độc hại mới.

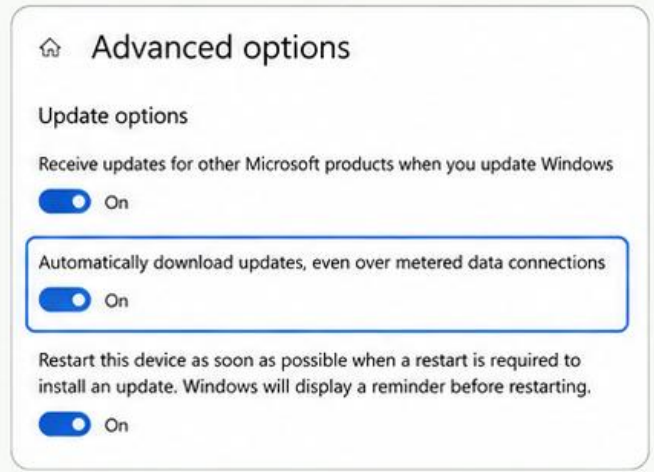
LƯU Ý: Hãy bật tính năng cập nhật tự động để luôn nhận được các bản cập nhật mới nhất.

Hướng dẫn thiết lập cập nhật tự động trên Windows 10/11

01

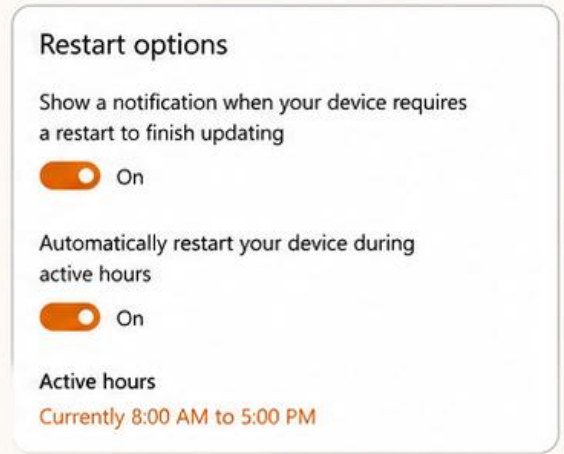
Vào mục **Settings**, chọn **Update & Security** (hoặc **Windows Update**).

02



Chọn mục **Advanced options**, bật tính năng tự động tải và cài đặt bản cập nhật.

03



Đồng ý khởi động lại máy tính khi có yêu cầu hoàn tất cài đặt bản cập nhật.

LƯU Ý

Windows sẽ tự động kiểm tra, tải về và cài đặt các bản cập nhật quan trọng để bảo vệ thiết bị và cải thiện hiệu suất.

Nguy cơ từ hệ điều hành Windows không bản quyền

- **Sử dụng các bản Windows crack** hoặc các phần mềm bẻ khóa tải từ mạng xã hội.

- **Các công cụ crack** thường chứa sẵn mã độc Trojan cài cắm vào sâu trong hệ điều hành.

- **Tính năng Windows Update** thường bị tắt để tránh phát hiện bản quyền giả.

- **Máy tính sẽ hoàn toàn mất khả năng tự bảo vệ** trước các mối đe dọa mới.

LƯU Ý:

Hãy luôn sử dụng **Windows bản quyền** để đảm bảo an toàn, ổn định và nhận được các bản cập nhật bảo mật mới nhất từ Microsoft.

Phần 2 - Kết nối an toàn với USB và Wi-Fi công cộng

01 **Các hiểm họa lây nhiễm virus** từ thiết bị lưu trữ ngoại vi USB.

02 **Quy tắc sử dụng thiết bị USB an toàn** tại công sở.

03 **Các nguy cơ mất an toàn** khi kết nối mạng Wi-Fi công cộng.

04 **Cách thiết lập kết nối mạng an toàn** để bảo vệ dữ liệu.

Hiểm họa lây nhiễm mã độc qua thiết bị USB di động

01 **Ổ đĩa USB** là vật trung gian truyền dẫn virus phổ biến nhất giữa các máy tính trong cơ quan.

02 **Virus tự động** sao chép mã độc vào USB khi cắm vào máy tính bị nhiễm.

03 **Khi cắm USB** đó sang máy tính sạch, virus sẽ lây lan sang máy mới.

LƯU Ý: Luôn quét virus cho USB trước khi sử dụng và không cắm các USB không rõ nguồn gốc để bảo vệ hệ thống và dữ liệu của bạn.

Cơ chế tự động chạy (AutoPlay/AutoRun) và virus USB

01

Tính năng **AutoPlay** của Windows tự động mở thư mục hoặc chạy file nhạc, phim khi cắm USB.

02

Hacker lợi dụng tính năng này để **buộc hệ thống chạy tệp tin chứa virus** ẩn trong USB ngay khi vừa cắm thiết bị vào máy.

Khuyến nghị - Cần tắt tính năng **AutoPlay** trên hệ điều hành Windows.

LƯU Ý:

- Luôn quét virus cho USB trước khi mở hoặc chạy bất kỳ tệp tin nào.
- Không mở các tệp tin lạ, không rõ nguồn gốc từ USB.
- Sao lưu dữ liệu quan trọng thường xuyên để phòng tránh rủi ro.

Virus ẩn tệp tin và tạo phím tắt giả mạo trong USB

01

Đây là loại virus USB **phổ biến** tại các cơ quan nhà nước **địa phương**.

02

Virus sẽ ẩn toàn bộ các thư mục chứa **tài liệu thật** của người dùng trong USB.

03

Tạo ra các **phím tắt giả mạo (Shortcut)** có tên giống hệt thư mục cũ.

04

Khi người dùng bấm vào phím tắt để mở tài liệu, virus sẽ **lập tức được chạy**.

LƯU Ý:

- Luôn bật hiển thị file ẩn và phần mở rộng file.
- Không mở phím tắt từ USB khi chưa kiểm tra bằng phần mềm diệt virus.
- Quét virus cho USB trước khi mở hoặc sao chép dữ liệu.

Quy tắc sử dụng USB an toàn tại cơ quan làm việc

01

Không sử dụng các ổ USB **lạ**, USB nhặt được hoặc **không rõ nguồn gốc**.

02

Quét virus toàn bộ ổ đĩa USB bằng phần mềm diệt virus trước khi mở.

03

Tắt tính năng tự động chạy **AutoPlay** của USB trong mục cài đặt Windows.

04

Bật thể thị **tệp tin ẩn** để phát hiện các file phím tắt lạ có đuôi **'.lnk'** hoặc **'.exe'**.

LƯU Ý:

Tuân thủ các quy tắc trên giúp bảo vệ hệ thống, dữ liệu và đảm bảo an toàn thông tin cho cơ quan.

Rủi ro mất an toàn khi sử dụng mạng Wi-Fi công cộng

01

Mạng Wi-Fi tại quán cà phê, sân bay, khách sạn
thường không cấu hình mật khẩu hoặc dùng chung một mật khẩu.

02

Dữ liệu truyền qua các mạng này không được mã hóa,
dễ bị kẻ xấu thu thập.

03

Nguy cơ mất thông tin tài khoản
đăng nhập và nội dung tài liệu giao dịch.

KHUYẾN NGHỊ

- Hạn chế truy cập tài khoản quan trọng khi dùng Wi-Fi công cộng.
- Ưu tiên sử dụng VPN để mã hóa dữ liệu khi bắt buộc phải kết nối.
- Luôn đăng xuất sau khi sử dụng và quên mạng Wi-Fi khi không cần thiết.

Kỹ thuật nghe lén thông tin truyền qua mạng (Eavesdropping)

01

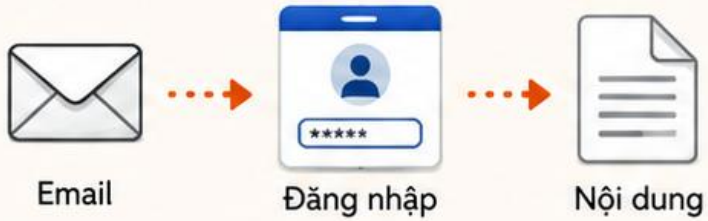
Kẻ xấu kết nối vào cùng một mạng Wi-Fi công cộng

Kẻ tấn công kết nối vào cùng một mạng Wi-Fi công cộng với người dùng.

02

Sử dụng các phần mềm bắt gói tin để đọc trộm

Sử dụng các phần mềm bắt gói tin để đọc trộm toàn bộ dữ liệu truyền nhận từ máy của người dùng.



03

Có thể thu thập được mật khẩu, email và nội dung văn bản chưa mã hóa.

Kẻ tấn công có thể thu thập thông tin nhạy cảm như mật khẩu, email, nội dung trò chuyện, thông tin thẻ tín dụng, v.v.

KHUYẾN NGHỊ

Ưu tiên sử dụng **HTTPS** khi truy cập website.

Sử dụng **VPN** để mã hóa dữ liệu truyền qua mạng.

Tránh kết nối Wi-Fi công cộng khi thực hiện giao dịch quan trọng.

Cập nhật và sử dụng **phần mềm diệt virus, tường lửa.**

Trạm phát Wi-Fi giả mạo và nguy cơ bị hack tài khoản

01

Kẻ xấu thiết lập một điểm phát Wi-Fi miễn phí không cần mật khẩu.

02

Đặt tên trùng hoặc gần giống với Wi-Fi của cơ quan hoặc địa điểm công cộng (ví dụ `Wifi_Mien_Phi`).

03

Khi người dùng kết nối vào, mọi lưu lượng mạng sẽ đi qua máy tính của kẻ xấu để phân tích lấy thông tin.

KHUYẾN NGHỊ

- Không kết nối Wi-Fi miễn phí không rõ nguồn gốc.
- Luôn truy cập website có HTTPS (biểu tượng ổ khóa trên trình duyệt).
- Bật xác thực 2 lớp (2FA) cho các tài khoản quan trọng.
- Hạn chế truy cập tài khoản nhạy cảm khi dùng Wi-Fi công cộng.

Hướng dẫn kết nối Wi-Fi công cộng an toàn

01

Tắt tính năng tự động kết nối Wi-Fi

Tắt tính năng tự động kết nối Wi-Fi trên điện thoại và máy tính xách tay để tránh kết nối vào mạng không mong muốn.

02

Hạn chế đăng nhập tài khoản quan trọng

Hạn chế thực hiện đăng nhập vào tài khoản công vụ hoặc giao dịch ngân hàng khi dùng mạng công cộng.

03

Đảm bảo truy cập website dùng HTTPS

Đảm bảo trang web truy cập sử dụng giao thức bảo mật HTTPS (có biểu tượng ổ khóa màu xanh lá trên thanh địa chỉ).

LƯU Ý

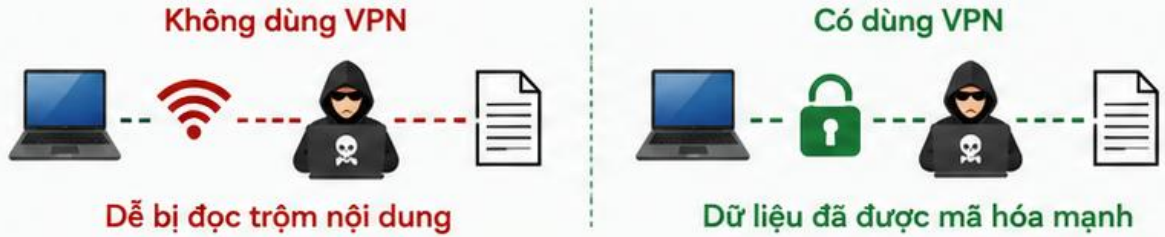
- Chỉ kết nối Wi-Fi công cộng từ các địa điểm uy tín.
- Sử dụng VPN để mã hóa dữ liệu khi cần thiết.
- Không truy cập các trang web lạ hoặc chứa nội dung nhạy cảm.
- Đăng xuất khỏi tài khoản sau khi sử dụng.

Khái niệm Mạng riêng ảo (VPN) và cơ chế mã hóa dữ liệu

01

VPN tạo ra một đường ống bảo mật được mã hóa

VPN tạo ra một đường ống bảo mật được mã hóa giữa máy tính người dùng và internet.



02

Dù kẻ xấu có bắt được các gói tin truyền qua Wi-Fi công cộng,

chúng cũng không thể đọc được nội dung do đã được mã hóa mạnh.

03

Khuyến nghị - Sử dụng dịch vụ VPN tin cậy

Sử dụng dịch vụ VPN tin cậy khi bắt buộc phải làm việc qua mạng công cộng để bảo vệ dữ liệu cá nhân, tài khoản và thông tin quan trọng.

KHUYẾN NGHỊ

- Chọn dịch vụ VPN uy tín (không miễn phí, không rõ nguồn gốc).
- Luôn bật VPN khi kết nối Wi-Fi công cộng.
- Tránh truy cập các trang web không sử dụng HTTPS.
- Kết hợp với xác thực 2 lớp (2FA) để bảo vệ tài khoản tốt hơn.
- Cập nhật phần mềm và hệ điều hành thường xuyên.

Hạn chế thực hiện giao dịch nhạy cảm qua Wi-Fi công cộng

01

Tránh chuyển khoản ngân hàng, mua sắm trực tuyến bằng thẻ tín dụng.

Những giao dịch này có thể bị kẻ xấu đánh cắp thông tin thẻ, mã OTP và chiếm đoạt tài sản.

02

Tránh đăng nhập vào hệ thống thư điện tử công vụ hoặc hệ thống quản lý văn bản nội bộ.

Nguy cơ bị đánh cắp tài khoản, đọc trộm email và dữ liệu quan trọng của cơ quan, tổ chức.

03

Tránh thay đổi mật khẩu của các tài khoản quan trọng.

Kẻ xấu có thể chặn dữ liệu để biết mật khẩu mới, gây mất quyền kiểm soát tài khoan của bạn.

KHUYẾN NGHỊ AN TOÀN

- Sử dụng VPN để mã hóa dữ liệu khi kết nối Wi-Fi công cộng.
- Kiểm tra kỹ địa chỉ website (bắt đầu bằng https://).
- Đăng xuất sau khi sử dụng các dịch vụ trực tuyến.
- Không lưu mật khẩu, không chọn "Ghi nhớ trên trình duyệt.
- Cập nhật hệ điều hành, trình duyệt và phần mềm diệt virus thường xuyên.

Sử dụng mạng 4G/5G cá nhân làm giải pháp thay thế an toàn

01

Mạng dữ liệu di động 4G/5G của các nhà mạng viễn thông được **mã hóa ở cấp độ thuê bao di động.**

02

Có độ an toàn cao hơn rất nhiều so với mạng Wi-Fi công cộng.

03

Nên bật tính năng điểm phát sóng cá nhân (Hotspot) trên điện thoại để chia sẻ mạng cho máy tính xách tay làm việc khi đi công tác.

KHUYẾN NGHỊ

- Sử dụng SIM chính chủ, gói cước 4G/5G của nhà mạng uy tín.
- Cập nhật phần mềm điện thoại thường xuyên để vá lỗ hổng bảo mật.
- Giám sát lưu lượng dữ liệu để tránh phát sinh chi phí.
- Không mở các liên kết lạ, không tải ứng dụng không rõ nguồn gốc.

Phần 3 - Quy trình sao lưu và bảo vệ dữ liệu văn phòng

01 Sự cần thiết của việc phân loại thông tin tài liệu.

- Giúp xác định mức độ quan trọng của dữ liệu.
- Áp dụng chính sách bảo vệ phù hợp.
- Ưu tiên sao lưu và bảo vệ dữ liệu quan trọng.

Phân loại dữ liệu

QUAN TRỌNG

- Tài chính – Kế toán
- Hợp đồng, pháp lý
- Dữ liệu khách hàng

NỘI BỘ

- Tài liệu nhân sự
- Quy trình, báo cáo
- Kế hoạch công việc

CÔNG KHAI

- Tài liệu chia sẻ
- Thông tin giới thiệu
- Tài liệu công khai

02 Kỹ thuật mã hóa file văn bản bằng phần mềm nén thông dụng.

- Mã hóa giúp bảo vệ dữ liệu khi lưu trữ hoặc truyền qua mạng.
- Sử dụng mật khẩu mạnh và lưu giữ an toàn.

Quy trình mã hóa file (ví dụ với 7-Zip/WinRAR)

1. Chọn file/thư mục cần nén
2. Chuột phải > Add to archive…
3. Đặt mật khẩu mạnh (ít nhất 12 ký tự)
4. Chọn phương thức mã hóa AES-256 (nếu có)
5. Lưu file nén đã mã hóa

03 Chiến lược sao lưu dữ liệu chống ransomware khóa file.

- Sao lưu định kỳ, tách biệt và kiểm tra khôi phục.
- Tuân thủ quy tắc 3-2-1 để đảm bảo an toàn.

Quy tắc sao lưu 3-2-1

3 Có ít nhất 3 bản sao dữ liệu

+ **2** Lưu trên 2 loại thiết bị khác nhau

+ **1** Có 1 bản sao lưu ở vị trí khác (ngoại tuyến/offline hoặc cloud)

- Sao lưu định kỳ (hàng ngày/tuần).
- Ngắt kết nối bản sao lưu sau khi hoàn tất.
- Không lưu bản sao lưu trên cùng thiết bị.
- Thường xuyên kiểm tra khả năng khôi phục dữ liệu.

THỰC HÀNH TỐT NHẤT

- Sử dụng mật khẩu mạnh và không chia sẻ cho người khác.
- Cập nhật phần mềm nén và phần mềm diệt virus thường xuyên.
- Phân quyền truy cập dữ liệu theo nguyên tắc ít quyền nhất.
- Cảnh giác với email độc hại và tệp đính kèm không rõ nguồn gốc.
- Xây dựng quy trình sao lưu và khôi phục dữ liệu rõ ràng, định kỳ diễn tập.

Tại sao dữ liệu cơ quan cần được phân loại và bảo vệ?

Không phải tài liệu nào cũng có mức độ quan trọng như nhau.

Mỗi loại dữ liệu có giá trị và rủi ro khác nhau khi bị lộ, mất mát hoặc bị thay đổi.

Phân loại dữ liệu giúp tối ưu hóa chi phí và nguồn lực bảo vệ thông tin.

Tập trung nguồn lực cho dữ liệu quan trọng, tránh lãng phí và nâng cao hiệu quả bảo mật.

Đảm bảo tuân thủ các quy định của pháp luật về bảo vệ bí mật nhà nước.

Tránh vi phạm pháp luật, rủi ro pháp lý và các hình thức xử phạt.

PHÂN LOẠI DỮ LIỆU – BẢO VỆ PHÙ HỢP

MỨC ĐỘ	TỐI MẬT	MẬT	HẠN CHẾ	CÔNG KHAI
MÔ TẢ	Dữ liệu đặc biệt quan trọng, liên quan đến bí mật nhà nước, an ninh, quốc phòng...	Dữ liệu quan trọng, nếu lộ có thể ảnh hưởng nghiêm trọng đến hoạt động của cơ quan, tổ chức.	Dữ liệu nội bộ, phục vụ công việc của cơ quan, lộ có thể gây ảnh hưởng ở mức độ nhất định.	Dữ liệu được phép công bố ra bên ngoài theo quy định.
BIỆN PHÁP BẢO VỆ	• Mã hóa bắt buộc • Hạn chế truy cập nghiêm ngặt • Lưu trữ và truyền qua kênh an toàn • Sao lưu ngoại tuyến	• Kiểm soát truy cập • Mã hóa khi truyền/lưu trữ • Sao lưu định kỳ • Giám sát và ghi nhật ký truy cập	• Phân quyền truy cập • Sao lưu định kỳ • Bảo vệ bằng mật khẩu • Cập nhật và vá lỗi thường xuyên	• Đảm bảo tính chính xác • Kiểm tra trước khi công bố • Công bố trên kênh chính thức • Theo dõi và phản hồi

THỰC HÀNH TỐT

- Xác định dữ liệu và phân loại ngay từ đầu.
- Nâng cao nhận thức và đào tạo cho cán bộ, nhân viên.
- Xây dựng và cập nhật quy định, quy trình nội bộ.
- Kiểm tra, đánh giá và cải tiến định kỳ.
- Báo cáo và xử lý kịp thời các sự cố rò rỉ, mất mát dữ liệu.

3 cấp độ phân loại tài liệu tại cơ quan hành chính

01 TÀI LIỆU THÔNG THƯỜNG

Văn bản pháp luật công khai, thông cáo báo chí, lịch công tác chung.

VÍ DỤ

- Văn bản pháp luật, văn bản hướng dẫn được công khai
- Thông cáo báo chí, thông tin tuyên truyền
- Lịch công tác chung, thông báo chung

YÊU CẦU BẢO VỆ

- Công khai, dễ dàng truy cập
- Sao lưu định kỳ
- Lưu trữ theo thời hạn quy định

02 TÀI LIỆU NỘI BỘ

Báo cáo tiến độ công việc, quy trình nghiệp vụ nội bộ của đơn vị.

VÍ DỤ

- Báo cáo tiến độ, kết quả công việc
- Quy trình, quy định nghiệp vụ nội bộ
- Kế hoạch, dự thảo văn bản chưa ban hành
- Tài liệu đào tạo nội bộ

YÊU CẦU BẢO VỆ

- Chỉ sử dụng trong nội bộ đơn vị
- Phân quyền truy cập
- Mã hóa khi lưu trữ và truyền tải
- Không chia sẻ ra bên ngoài khi chưa được phép

03 TÀI LIỆU BÍ MẬT

Văn bản có dấu mật, thông tin cá nhân của người dân, tài liệu chiến lược.

VÍ DỤ

- Văn bản, tài liệu có dấu mật (Tối mật, Mật, Tối mật)
- Thông tin cá nhân, dữ liệu công dân
- Tài liệu chiến lược, kế hoạch trọng yếu
- Dữ liệu tài chính, thông tin nhạy cảm

YÊU CẦU BẢO VỆ

- Hạn chế chặt chẽ người truy cập
- Mã hóa, xác thực mạnh
- Lưu trữ an toàn, tách biệt
- Không sao chép, không chuyển ra ngoài
- Giám sát, ghi nhật ký truy cập

LƯU Ý CHUNG: Việc phân loại tài liệu giúp quản lý, lưu trữ, chia sẻ và bảo vệ thông tin hiệu quả, đáp ứng yêu cầu pháp luật và đảm bảo an toàn thông tin cho cơ quan, tổ chức.

- Tuân thủ pháp luật
- Bảo vệ thông tin
- Nâng cao hiệu quả
- Tăng cường uy tín

Nguyên tắc lưu trữ và trao đổi tài liệu mật đúng quy định

01

Tuyệt đối không lưu trữ tài liệu mật trên máy tính kết nối Internet công cộng.

Chỉ lưu trữ trên thiết bị và hệ thống được cấp phép, quản lý của cơ quan.

VÌ SAO?

Máy tính kết nối Internet công cộng có nguy cơ bị tấn công, đánh cắp dữ liệu.
Dễ bị cài mã độc, theo dõi và lộ lọt thông tin.

02

Không gửi tài liệu mật qua các ứng dụng chat như Zalo, Viber hay Facebook.

Các ứng dụng này không đảm bảo mã hóa đầu cuối theo quy định.

VÌ SAO?

Dữ liệu có thể bị bên thứ ba truy cập.
Tài khoản có thể bị chiếm đoạt.
Không tuân thủ quy định bảo vệ bí mật nhà nước.

03

Sử dụng các hệ thống mạng truyền số liệu chuyên dùng của Đảng, Nhà nước để gửi tài liệu mật.

Tuân thủ đúng quy trình, phân quyền và kiểm soát khi truyền gửi, tiếp nhận tài liệu mật.

VÌ SAO?

Hệ thống chuyên dùng được thiết kế, quản lý, giám sát và có khả năng mã hóa, xác thực cao.
Đảm bảo an toàn, bảo mật theo quy định của pháp luật.

LƯU Ý CHUNG

- Chỉ lưu trữ tài liệu mật trên thiết bị, hệ thống được cấp phép.
- Mã hóa và phân quyền truy cập theo nguyên tắc "cần biết" và "ít nhất".
- Kiểm tra, rà soát và xóa dữ liệu mật theo thời hạn quy định.
- Bảo vệ thiết bị, tài khoản bằng mật khẩu mạnh, xác thực 2 lớp.
- Phát hiện vi phạm phải báo cáo ngay cho cấp có thẩm quyền.

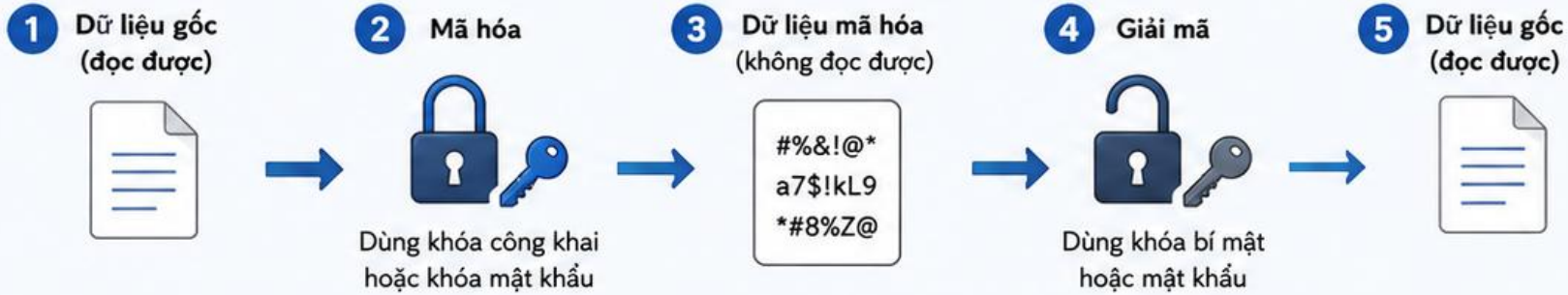
Khái niệm mã hóa dữ liệu cơ bản

Là quá trình biến đổi dữ liệu
từ dạng đọc được sang dạng không thể đọc được nếu không có khóa giải mã.

Giúp bảo vệ dữ liệu an toàn
ngay cả khi tệp tin bị kẻ xấu sao chép trái phép.

Có thể thực hiện mã hóa dễ dàng
bằng các phần mềm nên tệp tin thông dụng.

Quy trình mã hóa và giải mã

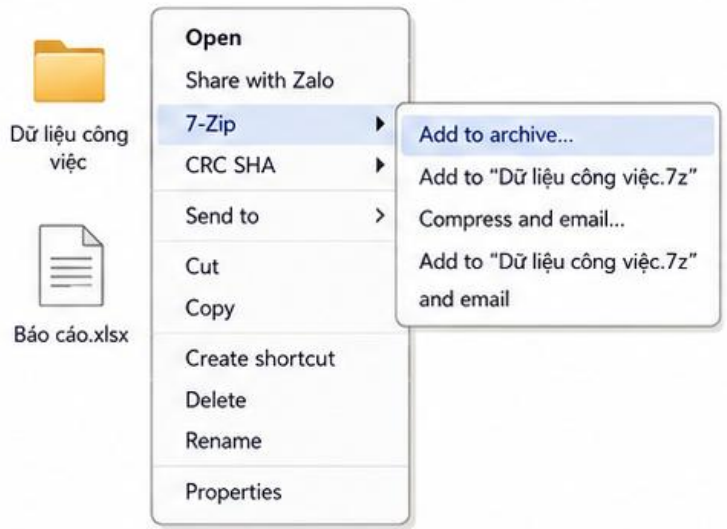


Lưu ý quan trọng

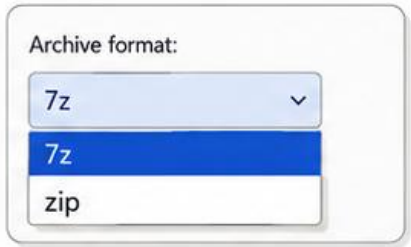
- Bảo quản khóa/mật khẩu cẩn thận.
- Không chia sẻ khóa hoặc mật khẩu.
- Luôn cập nhật phần mềm mã hóa.
- Mã hóa kết hợp với sao lưu để bảo vệ dữ liệu tối đa.

Hướng dẫn nén và mã hóa tệp tin bằng phần mềm 7-Zip

1 Nhấp chuột phải vào tệp tin hoặc thư mục cần mã hóa, chọn 7-Zip và Add to archive.



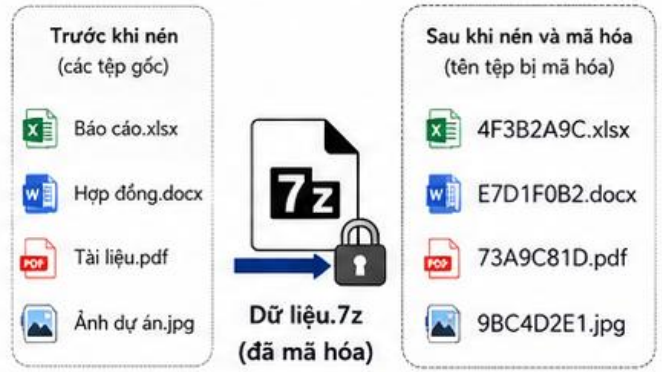
2 Chọn định dạng nén là '7z' hoặc 'zip'.



Khuyến nghị:
Chọn định dạng '7z' để đạt tỷ lệ nén tốt hơn và bảo mật cao hơn.

3 Tại mục Encryption, nhập mật khẩu bảo vệ và chọn thuật toán mã hóa 'AES-256'.

4 Tích chọn ô Encrypt file names để mã hóa cả tên của các tệp tin bên trong.



Khi mở tệp nén, 7-Zip sẽ yêu cầu mật khẩu để giải mã và truy cập dữ liệu.

LƯU Ý QUAN TRỌNG

- Sử dụng mật khẩu mạnh: tối thiểu 12 ký tự, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.
- Lưu mật khẩu ở nơi an toàn, không chia sẻ cho người không có thẩm quyền.
- Luôn cập nhật phiên bản 7-Zip mới nhất để đảm bảo an toàn.
- Sao lưu tệp nén ở nhiều vị trí khác nhau để phòng trường hợp mất dữ liệu.

Quy tắc chia sẻ mật khẩu file an toàn qua kênh thứ hai

1

Khi gửi tệp tin đã mã hóa cho đồng nghiệp qua Email công vụ.

Luôn mã hóa tệp tin trước khi gửi và chỉ gửi từ địa chỉ Email công vụ.

2

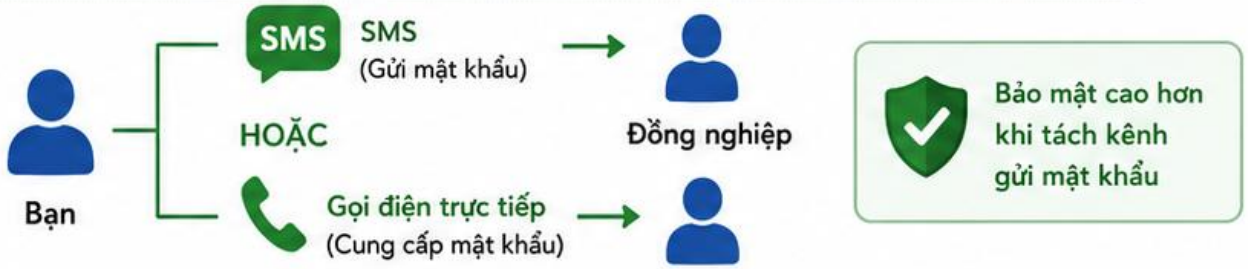
Tuyệt đối không gửi kèm mật khẩu giải nén trong cùng một email đó.

Việc này làm tăng rủi ro lộ lọt thông tin nếu email bị đánh cắp.

3

Hãy sử dụng một kênh liên lạc thứ hai để gửi mật khẩu giải nén

(ví dụ nhắn tin SMS qua số điện thoại hoặc gọi điện trực tiếp).



LƯU Ý QUAN TRỌNG

- Mật khẩu nên đủ mạnh: tối thiểu 12 ký tự, kết hợp chữ hoa, chữ thường, số và ký tự đặc biệt.
- Chỉ cung cấp mật khẩu cho đúng người nhận.
- Xóa tin nhắn SMS hoặc email chứa mật khẩu sau khi người nhận đã giải nén thành công.
- Không chia sẻ mật khẩu qua các kênh không an toàn (mạng xã hội, ứng dụng chat không bảo mật...).

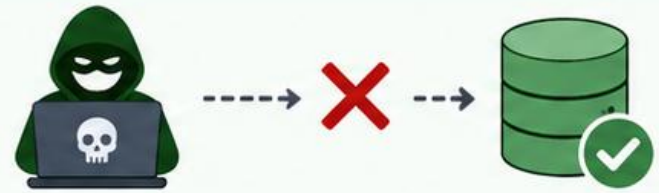
Tầm quan trọng của việc sao lưu dữ liệu thường xuyên

Dữ liệu có thể bị mất do hỏng ổ cứng máy tính, cháy nổ thiết bị.

- Sao lưu giúp khôi phục dữ liệu khi xảy ra sự cố bất ngờ.

Máy tính bị nhiễm mã độc tống tiền khóa dữ liệu, đòi tiền chuộc.

- Dữ liệu sao lưu giúp phục hồi mà không phải trả tiền chuộc.



Cán bộ vô tình xóa nhầm hoặc ghi đè lên tài liệu gốc quan trọng.

- Sao lưu giúp khôi phục lại phiên bản dữ liệu đã mất.

Sao lưu dự phòng là phương pháp hiệu quả nhất để tự bảo vệ tài liệu làm việc.

- Giúp công việc không bị gián đoạn khi có sự cố.
- Tiết kiệm thời gian, chi phí và bảo đảm tính liên tục của hoạt động.

KẾT LUẬN: Sao lưu dữ liệu thường xuyên là thói quen quan trọng và cần thiết để bảo vệ dữ liệu, giảm thiểu rủi ro và bảo đảm an toàn thông tin trong mọi tình huống.

Chiến lược sao lưu dữ liệu theo nguyên tắc 3-2-1

Quy tắc đơn giản nhưng hiệu quả giúp bảo vệ dữ liệu trước mọi sự cố: mất mát, hỏng hóc, ransomware, thiên tai...

3 – Có ít nhất 3 bản sao của dữ liệu quan trọng

(1 bản gốc làm việc và 2 bản sao lưu).

1 bản gốc làm việc
(trên máy tính)

+

1 bản sao lưu thứ nhất

+

1 bản sao lưu thứ hai

Tổng cộng 3 bản sao

2 – Lưu trữ bản sao lưu trên ít nhất 2 loại phương tiện vật lý khác nhau

(ổ cứng máy tính và ổ cứng di động).

Loại 1:
Ổ cứng gắn trong (HDD/SSD)

← KHÁC LOẠI →

Loại 2:
Ổ cứng di động (HDD/SSD)

2 loại phương tiện lưu trữ khác nhau

1 – Có ít nhất 1 bản sao lưu được lưu trữ ở một địa điểm bên ngoài cơ quan

(trên đám mây công vụ hoặc cất giữ ổ cứng tại nhà).

Lưu trữ trên đám mây công vụ
(VNPT Cloud, Viettel IDC...)

HOẶC

Cất giữ ổ cứng tại nhà
(nơi an toàn, bảo mật)

Lưu trữ ngoài địa điểm cơ quan

LỢI ÍCH CỦA CHIẾN LƯỢC 3-2-1

- Giảm thiểu rủi ro mất dữ liệu.
- Khôi phục dữ liệu nhanh chóng.
- Đảm bảo tính liên tục của hoạt động.
- Tăng cường an toàn, bảo mật dữ liệu.
- Tuân thủ các tiêu chuẩn quản lý dữ liệu.

Phân biệt sao lưu cục bộ và sao lưu trên đám mây công vụ

Sao lưu cục bộ

Sao chép dữ liệu sang ổ cứng di động, USB hoặc phân vùng đĩa D/E. Tốc độ nhanh, dễ thực hiện nhưng dễ bị hỏng vật lý hoặc nhiễm virus lan truyền.

Các phương tiện lưu trữ

Ổ cứng di động

USB

Phân vùng đĩa D/E

Ưu điểm

Tốc độ sao lưu/khôi phục nhanh, dễ sử dụng, không phụ thuộc Internet.

Nhược điểm

Dễ hỏng vật lý, mất cắp, cháy nổ hoặc nhiễm virus lan truyền.

Phù hợp khi

Sao lưu ngắn hạn, dữ liệu không quá lớn, cần khôi phục nhanh tại chỗ.

Lưu ý

Cần bảo ngản cẩn thận, quét virus trước khi sử dụng.

Sao lưu đám mây công vụ

Đồng bộ dữ liệu lên hệ thống lưu trữ tập trung của tính. An toàn cao, có thể truy cập từ xa, có tính năng phục hồi phiên bản cũ của tệp tin.

Đặc điểm nổi bật

An toàn cao
Dữ liệu được mã hóa và lưu trữ tập trung, được bảo vệ nhiều lớp.

Truy cập từ xa
Truy cập mọi lúc, mọi nơi qua Internet bằng tài khoản được cấp quyền.

Phục hồi phiên bản
Có thể khôi phục lại các phiên bản cũ của tệp tin.

Ưu điểm

An toàn, không lo mất mát vật lý, khôi phục linh hoạt, mở rộng dễ dàng.

Nhược điểm

Phụ thuộc Internet, có thể phát sinh chi phí lưu trữ.

Phù hợp khi

Sao lưu dài hạn, dữ liệu quan trọng, phục vụ nhiều người dùng.

Lưu ý

Sử dụng tài khoản được cấp, đặt mật khẩu mạnh, bật xác thực 2 lớp.

KẾT HỢP CẢ HAI

Áp dụng nguyên tắc 3-2-1: có ít nhất 3 bản sao, lưu trữ trên ít nhất 2 loại phương tiện khác nhau, và có ít nhất 1 bản sao lưu ở địa điểm bên ngoài cơ quan.
Kết hợp sao lưu cục bộ và sao lưu đám mây giúp bảo vệ dữ liệu toàn diện và hiệu quả nhất.

Quy trình khôi phục dữ liệu khi gặp sự cố

1 Xác định mức độ mất mát dữ liệu và nguyên nhân gây ra sự cố.

- Thu thập thông tin sự cố.
- Xác định phạm vi ảnh hưởng.
- Phân loại: mất, hỏng, xóa nhầm, lỗi phần cứng, tấn công mã độc, thiên tai...

2 Nếu do máy tính bị nhiễm virus, phải diệt sạch virus hoặc cài lại hệ điều hành trước khi tiến hành khôi phục dữ liệu để tránh dữ liệu mới bị nhiễm độc lại.

- Ngắt kết nối Internet và các thiết bị ngoài.
- Diệt sạch virus bằng phần mềm diệt virus uy tín.
- Cập nhật hệ thống và phần mềm.
- Nếu cần thiết, cài lại hệ điều hành.

3 Sao chép bản sao lưu gần nhất quay lại thư mục làm việc và kiểm tra tính toàn vẹn của dữ liệu.

- Xác định bản sao lưu gần nhất phù hợp.
- Khôi phục dữ liệu vào thư mục làm việc.
- Kiểm tra tính toàn vẹn và tính đầy đủ của dữ liệu.

LƯU Ý QUAN TRỌNG

- Không ghi đè dữ liệu mới lên khu vực dữ liệu bị mất trước khi khôi phục.
- Luôn ưu tiên sử dụng bản sao lưu hợp lệ và đã được kiểm tra.
- Ghi chép lại quá trình xử lý, các bước thực hiện và kết quả để phục vụ kiểm tra, rút kinh nghiệm.
- Sau khi khôi phục, nên sao lưu lại ngay để đảm bảo an toàn và tuân thủ nguyên tắc 3-2-1.

CẢM ƠN VÀ THẢO LUẬN BUỔI 2