SỞ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

TẬP HUẤN

BỒI DƯỠNG KIẾN THỨC VỀ AN TOÀN, AN NINH THÔNG TIN

Quảng ngãi, năm 2023

VAI TRÒ CỦA ATTT TRONG CHUYỂN ĐỔI SỐ

- Chuyển đổi số tạo ra một không gian sống mới, gọi là không gian mạng hoặc môi trường số
- Chuyển đổi số phải an toàn, nhân văn và rộng khắp
- Bảo đảm an toàn, an ninh thông tin là then chốt, đảm bảo sự thành công của chuyển đổi số

MỘT SỐ VÍ DỤ CÁC CUỘC TẤN CÔNG LỚN

- Năm 2014, sau sự kiện giàn khoan HD 981 hạ đặt trái phép trong vùng đặc quyền kinh tế Việt Nam, tin tặc nước ngoài đã tấn công hơn 700 trang mạng Việt Nam và hơn 400 trang trong dịp Quốc khánh (2/9) để chèn các nội dung xuyên tạc chủ quyền của Việt Nam với quần đảo Hoàng Sa.
- năm 2016 là cuộc tấn công mạng vào một số màn hình hiển thị thông tin chuyến bay tại khu vực làm thủ tục chuyến bay của các sân bay quốc tế Tân Sơn Nhất, sân bay quốc tế Nội Bài, sân bay quốc tế Đà Nẵng, sân bay Phú Quốc. Các màn hình của sân bay đã bị chèn những hình ảnh và nội dung xuyên tạc về biển Đông.
- Thông tin từ bảng tổng kết an ninh mạng năm 2022 và dự báo 2023 do Bkav thực hiện. Theo đó, trong năm 2022, thiệt hại do virus máy tính gây ra đối với người dùng Việt Nam ở mức 21,2 nghìn tỷ đồng

TÌNH HÌNH ATTT 6 THÁNG ĐẦU NĂM 2023

- Trong 6 tháng đầu năm 2023, Cục An toàn thông tin đã ghi nhận, cảnh báo và hướng dẫn xử lý 6.362 cuộc tấn công mạng gây ra sự cố vào các hệ thống thông tin tại Việt Nam
- Riêng trong tháng 3/2023, Cục An toàn thông tin (ATTT) đã ghi nhận, cảnh báo và hướng dẫn xử lý 525 cuộc tấn công mạng (407 cuộc phishing, 65 cuộc deface, 53 cuộc malware) gây ra sự cố vào các hệ thống thông tin tại Việt Nam
- điều phối ngăn chặn 1.530 trang web/blog vi phạm pháp luật (559 trang lừa đảo trực tuyến)
- Các cuộc lừa đảo trực tuyến bùng phát

24 HÌNH THỨC LỪA ĐẢO TRỰC TUYẾN

- Vừa qua ngày 23/6/2023 bộ TTTT cảnh báo 24 hình thức lừa đảo trực tuyến

LỪA ĐẢO TUYỂN CỘNG TÁC VIÊN

LỪA ĐẢO CUỘC GỌI TỐNG TIỀN

LỪA ĐẢO VIEO DEEPFAKE

CÁC BIỆN PHÁP BẢO ĐẢM AN TOÀN THÔNG TIN

BIỆN PHÁP

1. An toàn máy tính cá nhân
2. An toàn khi sử dụng Internet
3. Phòng chống Virus
4. Sao lưu dữ liệu định kỳ

01

AN TOÀN MÁY TÍNH CÁ NHÂN

ĐẶT MẬT KHẨU AN TOÀN CHO MÁY TÍNH

- Mật khẩu phải khó đoán : Không bao gồm ngày tháng năm sinh… và những ký tự liền kề trên bàn phím máy tính QWER…,

- Phải tối thiểu từ 8 11 ký tự bao gồm cả chữ(chữ hoa và chữ thường), số, ký tự đặt biệt

- Không được ghi nhận mật khẩu vào bất kỳ phương tiện nào có thể truyền đạt thông tin(giấy, sổ tay…) trừ khi phương tiện đó được bảo vệ.

- Hạn chế sử dụng chung mật khẩu cho nhiều tài khoản khác nhau.

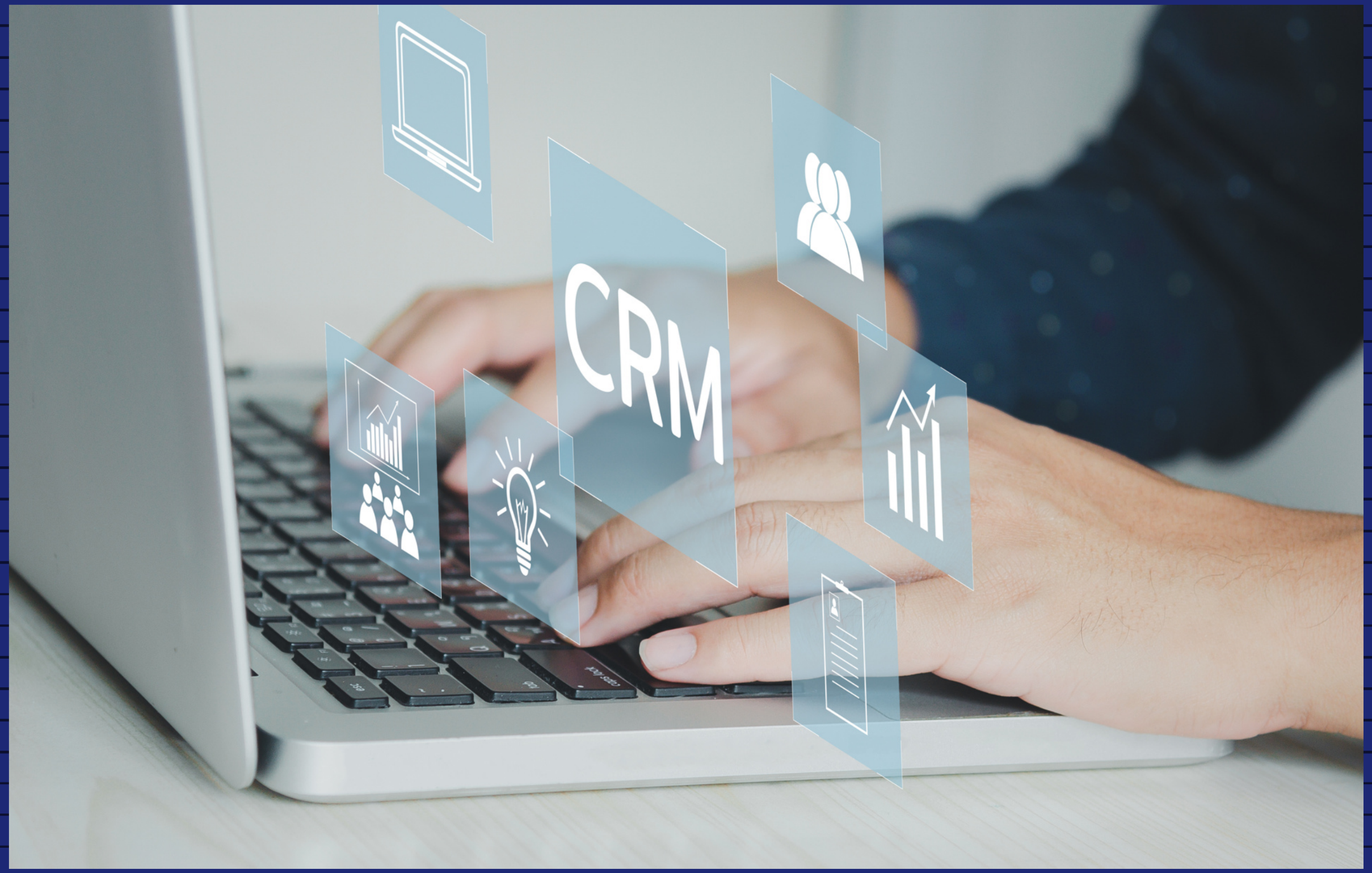
- Không sử dụng lại mật khẩu đã đặt trước đó.

ĐẶT MẬT KHẨU CHO TẬP TIN QUAN TRỌNG

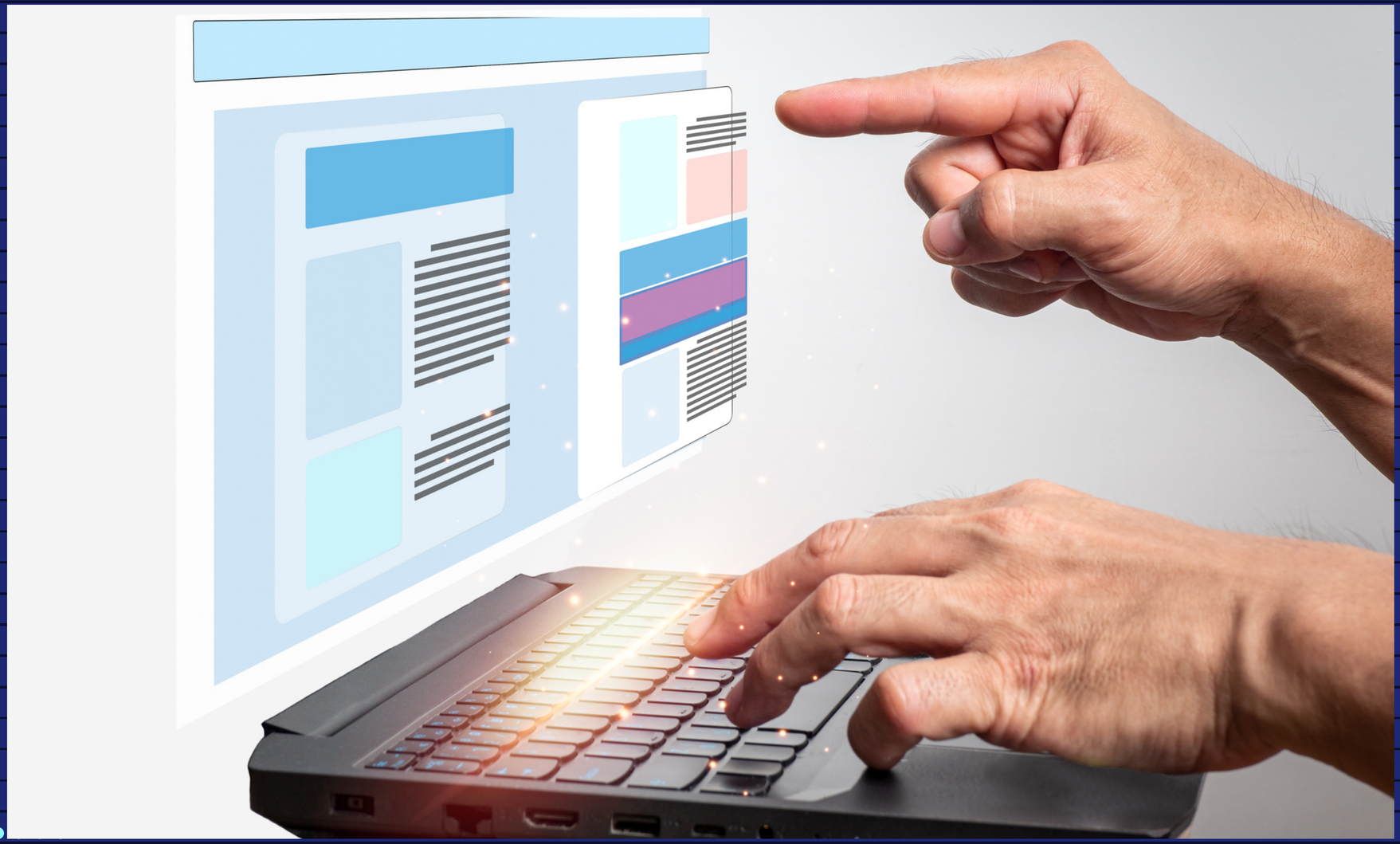
- Dùng để bảo vệ dữ liệu cá nhân của chính mình.
- Tránh trường hợp xoá nhầm Folder, File trên máy.
- Bảo mật những thông tin có tính chất nhạy cảm.
- Sử dụng phần mềm như 7-Zip, Winrar để đặt mật khẩu cho thư mục hoặc các tập tin quan trọng.

.....

SỬ DỤNG PHẦN MỀM CÓ BẢN QUYỀN



TẮT HOẶC GỠ BỎ NHỮNG PHẦN MỀM KHÔNG CẦN THIẾT



SỬ DỤNG USB AN TOÀN

AN TOÀN MÁY TÍNH CÁ NHÂN

BẬT CHẾ ĐỘ TƯỜNG LỬA

02

AN TOÀN KHI SỬ DỤNG INTERNET

AN TOÀN KHI SỬ DỤNG INTERNET

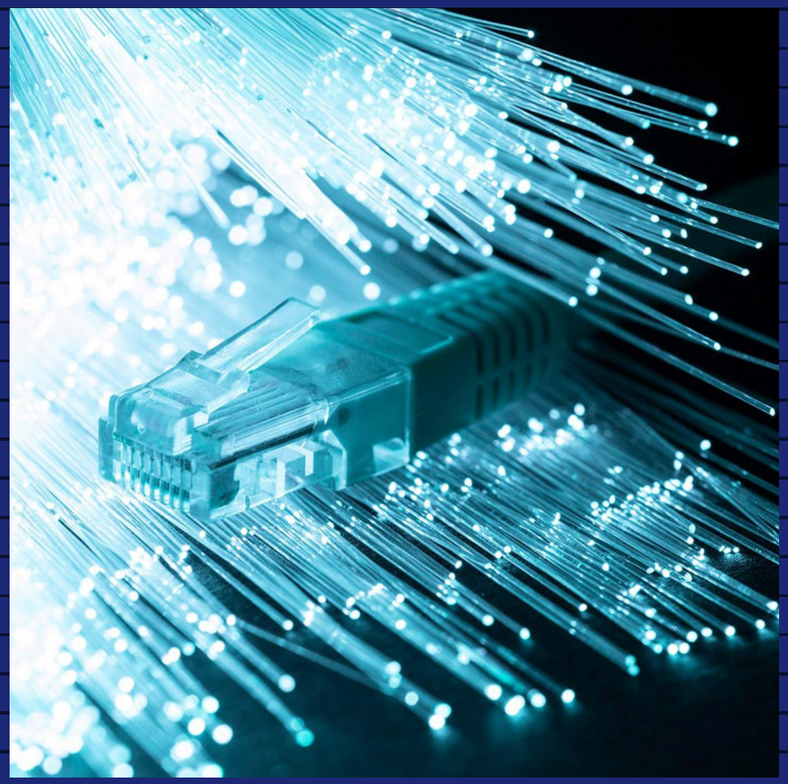
Internet ngày càng đóng vai trò quan trọng trong cuộc sống, đặt biệt là trong giai đoạn xu hướng chuyển đổi số đang ngày một phát triển.

Chính vì vậy Internet luôn tìm ẩn nguy cơ mất cấp dữ liệu cá nhân, trong khi ngày càng có nhiều thủ đoạn tinh vi của tội phạm mạng, luôn sẵn sàng xâm nhập và đánh chiếm thông tin cá nhân. Do đó việc trang bị các kiến thức để sử dụng Internet một cách an toàn là rất cần thiết.

AN TOÀN KHI SỬ DỤNG INTERNET

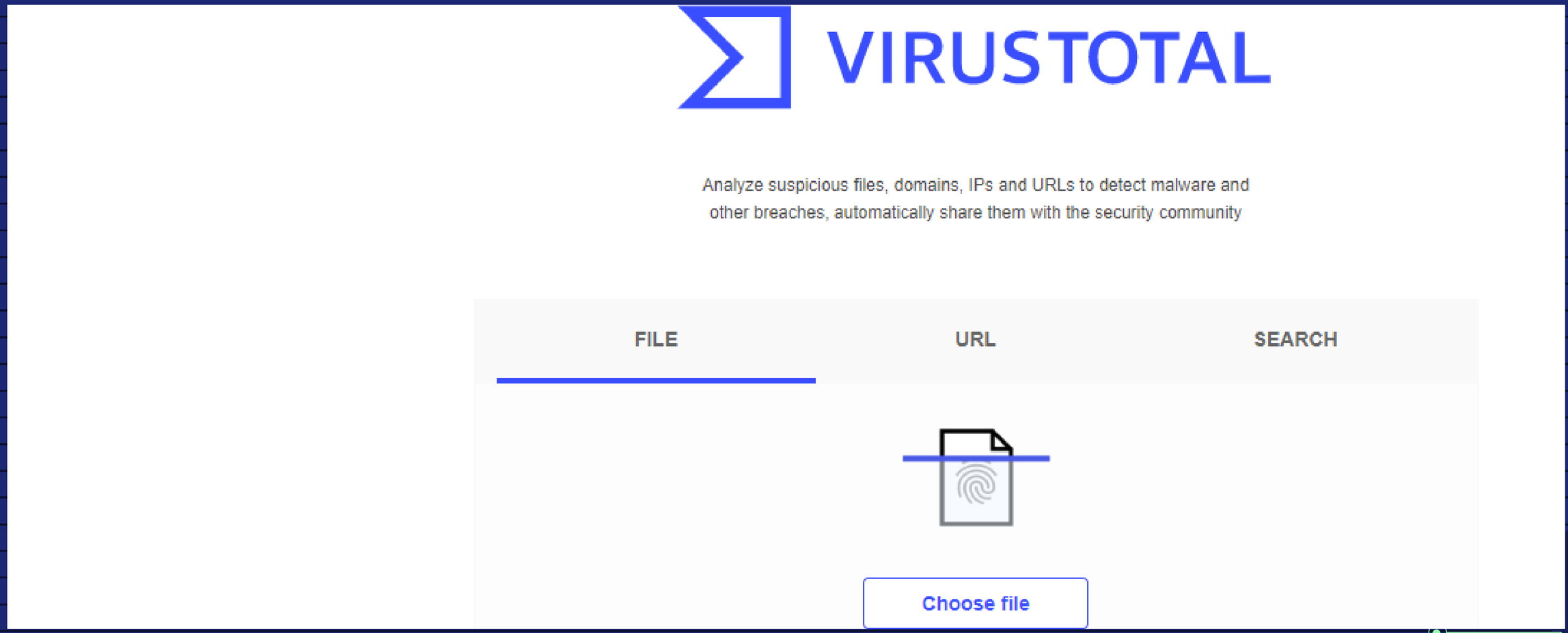
Những lưu ý khi sử dụng Internet:

- Quét Virus trước khi cài đặt và sử dụng trên các thiết bị.
- Không truy cập vào những trang web không rõ nguồn gốc, không an toàn.
- Không sử dụng các phần mềm Crack để mở khoá trái phép bản quyền hệ điều hành hoặc các ứng dụng.
- Luôn có một bản sao lưu dữ liệu dự phòng.



AN TOÀN KHI SỬ DỤNG INTERNET

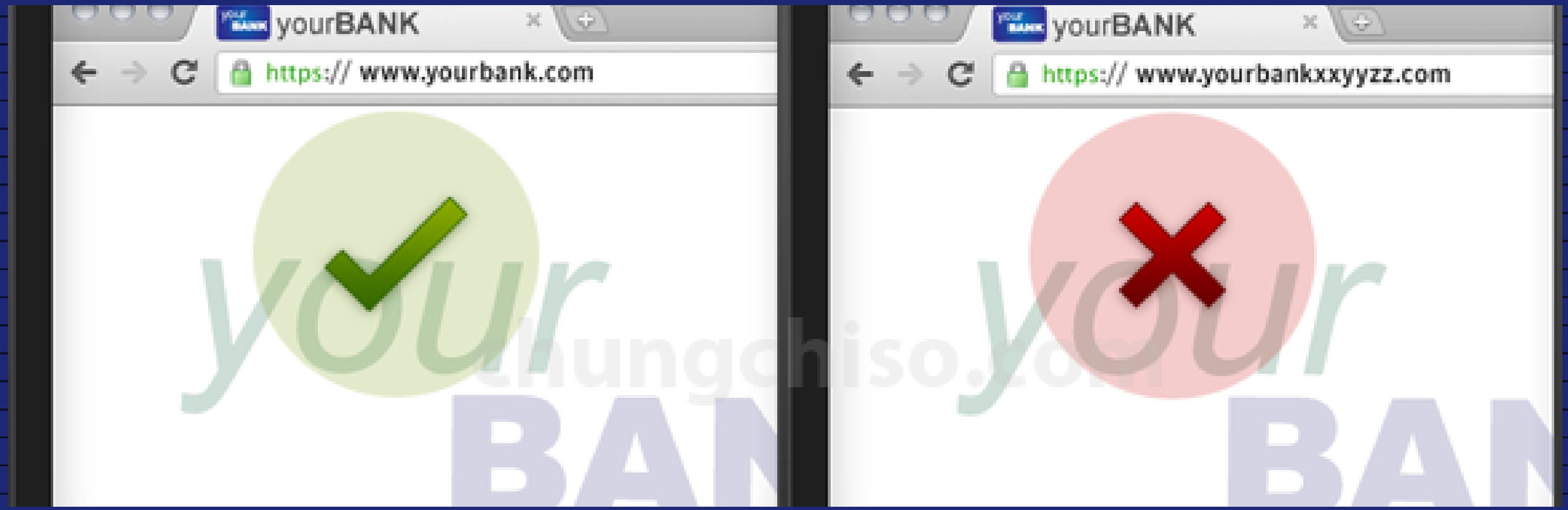
Quét Virus trước khi cài đặt và sử dụng trên các thiết bị giúp hạn chế tối đa những cuộc tấn công bảo mật hay tránh được tình trạng nhiễm virus trên máy tính.



AN TOÀN KHI SỬ DỤNG INTERNET

Dấu hiệu nhận biết một Website là uy tín, an toàn:

- Đầu tiên, URL trên thanh địa chỉ của trình duyệt phải bắt đầu bằng https:// và icon hình ổ khóa ở phía trước thanh địa chỉ .
- Luôn chú ý kiểm tra địa chỉ URL trên trình duyệt.



AN TOÀN KHI SỬ DỤNG INTERNET

- Lướt web ở chế độ ẩn danh
- Xử dụng email tạm thời để xác thực tài khoản (temp mail)
- Thận trong khi nhấp vào liên kết trong email
- Email có file đính kèm thì nên quét virus trước khi tải về
- Sử dụng kết nối VPN khi đăng nhập vào hệ thống

AN TOÀN KHI SỬ DỤNG INTERNET

Dấu hiệu nhận biết một Website là uy tín, an toàn:

- Trang web giả mạo thường sẽ ‘nhử’ mọi người bằng cách đưa ra những thông báo khiến mọi người quá hoảng sợ, hoặc quá vui mừng từ đó người dùng sẽ nhập vào username, mật khẩu theo yêu cầu của website.
- Ví dụ: "Theo quy trình kiểm tra định kỳ, chúng tôi cần bạn xác nhận lại thông tin cá nhân trên hệ thống. Xin vui lòng nhập vào username và mật khẩu để tiếp tục“

"Bạn đã được hệ thống chúng tôi lựa chọn ngẫu nhiên cho giải thưởng trị giá 100.000.000VND. Xin vui lòng nhập vào username và mật khẩu, thông tin thẻ tín dụng để chúng tôi xác nhận thông tin và chuyển tiền cho bạn"

AN TOÀN KHI SỬ DỤNG INTERNET

Hạn chế sử dụng những phần mềm Crack, mở khoá trái phép:

- Sử dụng phần mềm crack đồng nghĩa với việc vi phạm bản quyền, khi bị phát hiện sẽ phải chịu trách nhiệm về hành vi này.
- Khi sử dụng các phần mềm crack thì việc virus máy tính xâm nhập vào làm hỏng hệ thống máy tính, mất dữ liệu điều này sẽ gây thiệt hại rất lớn.
- Không nhận được các bản cập nhật, nâng cấp hay các bản vá lỗi từ nhà sản xuất.

03

PHÒNG CHỐNG VIRUS

PHÒNG CHỐNG VIRUS

Virus là thuật ngữ dùng để chỉ những đoạn mã chương trình được thiết kế để xâm nhập vào máy tính, nhằm mục đích lấy cắp thông tin, xóa dữ liệu, gửi email nặc danh, tự động nhân bản để lây lan sang các thiết bị khác.

Virus có thể lây nhiễm ở nhiều cách thức khác nhau và càng ngày càng tinh vi hơn.Những con đường lan truyền Virus chủ yếu và phổ biến nhất hiện nay:

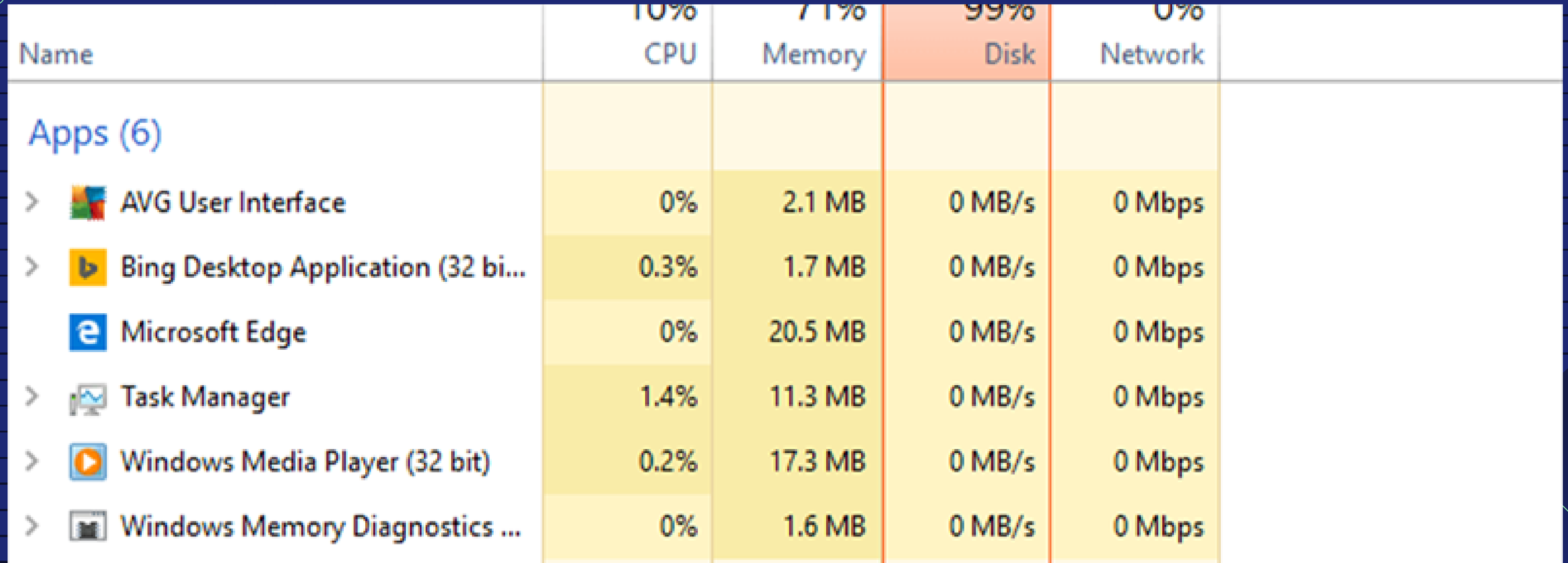
- Thiết bị gắn ngoài: USB, thẻ nhớ, ổ cứng di động….
- Lây truyền qua những trang web giả mạo.
- Virus lây nhiễm qua E-mail.
- Lây truyền qua mạng xã hội như FaceBoook, Zalo…

DẤU HIỆU NHẬN BIẾT THIẾT BỊ NHIỄM VIRUS

- Xuất hiện cảnh báo giả: trong quá trình sử dụng máy tính, thường xuyên xuất hiện nhữ
cửa sổ pop-up mặc dù bạn không có tác động gì đến những cửa sổ đó, gây cảm giác rất k
chịu trong quá trình sử dụng.

DẤU HIỆU NHẬN BIẾT THIẾT BỊ NHIỄM VIRUS

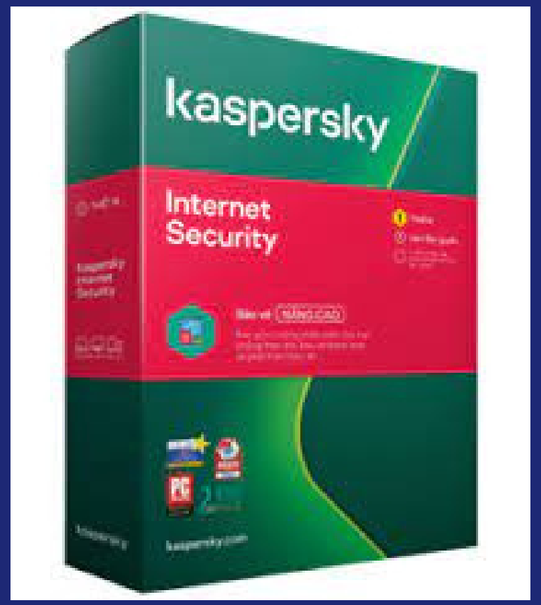
- - Máy hoạt động chậm một cách bất thường, tốc độ truy xuất, mở các tập tin chậm một cách đột ngột.
- - Không thể cài hoặc kích hoạt chức năng bảo vệ của phần mềm diệt virus.
- - Hoạt động đáng ngờ trên ổ cứng.



PHÒNG CHỐNG VIRUS

Những biện pháp phòng chống Virus:

- Khi cắm các thiết bị ngoại vi cần quét Virus trước khi mở file sử dụng.
- Tắt tính năng Auto Play trên hệ điều hành.
- Sử dụng tường lửa bảo mật trên hệ điều hành.
- Khuyến cáo sử dụng các phần mềm diệt Virus có bản quyền



04

SAO LƯU DỮ LIỆU ĐỊNH KỲ

SAO LƯU DỮ LIỆU ĐỊNH KỲ

Sao lưu dữ liệu là một biện pháp cần phải thực hiện để đảm bảo an toàn đối với các dữ liệu quan trọng. Sao lưu dữ liệu làm giảm nguy cơ đánh mất những file tài liệu, dữ liệu quan trọng.

Sao lưu dữ liệu là vô cùng cần thiết đối với tổ chức nói chung và cá nhân nói riêng. Dù đang sử dụng máy tính để bàn hay laptop hoặc đặc biệt là khi điều khi điều khiển cả một hệ thống máy chủ cho một cơ quan thì việc sao lưu dữ liệu luôn là nhiệm rất quan trọng.

SAO LƯU DỮ LIỆU ĐỊNH KỲ

Có 2 hình thức sao lưu dữ liệu chính: **Local Backup(sao lưu cục bộ)** và **Online Backup (sao lưu trực tuyến).** Sau đây chúng ta tìm hiểu cách thức hoạt động, điểm mạnh và điểm yếu của 2 hình thức này.

Hình thức 1: Local Backup

- Sử dụng các thiết bị rời: Ổ cứng, USB, DVD,…
- **Ưu điểm:** Lưu trữ nhanh, nhiều tùy chọn dung lượng, có thể sao lưu vào bất cứ thời điểm nào.
- **Nhược điểm:** Dễ bị hư hỏng, nhiễm virus từ thiết bị chính lúc sao lưu nếu không kiểm tra. Đặt biệt là ổ cứng rời hay usb thường xuyên hư hỏng do các tác động từ bên ngoài. Dung lượng lưu trữ cũng khá hạn chế.

SAO LƯU DỮ LIỆU ĐỊNH KỲ

Hình thức 2: Online Backup

- Sử dụng công nghệ điện toán đám mây để sao lưu dữ liệu.
- **Ưu điểm:** An toàn và tin cậy, có thể truy cập dữ liệu từ bất kì đâu, từ bất kì máy tính hoặc thiết bị di động nào miễn là có kết nối Internet. Chính vì những ưu điểm này đã giúp hình thức Online backup dần thay thế cho backup truyền thống.
- **Nhược điểm:** yêu cầu thiết bị phải có kết nối Internet và mất nhiều thời gian hơn(tùy thuộc vào đường truyền và dung lượng của File backup).

MỘT SỐ SỰ CỐ THƯỜNG GẶP TRÊN MÔI TRƯỜNG SỐ

- Bị nhiễm mã độc trên máy tính/ thiết bị thông minh
- Lộ lọt thông tin cá nhân
- Cài nhầm ứng dụng giả mạo
- Nhận email giả mạo
- Kết nối vào mạng wifi không an toàn
- Bị lừa đảo trực tuyến
- …

- CẦN TRANG BỊ CÁC KỸ NĂNG SỐ
- CẦN NGHIÊM TÚC THỰC HIỆN CÁC BIỆN PHÁP ĐẢM BẢO AN TOÀN THÔNG TIN MẠNG ĐƯỢC KHUYẾN CÁO
- LUÔN SAO LƯU DỮ LIỆU QUAN TRỌNG
- THEO DÕI VÀ CẬP NHẬT THÔNG TIN
- LIÊN HỆ KHI GẶP SỰ CỐ

GIẢI QUYẾT SỰ CỐ THƯỜNG GẶP TRÊN MÔI TRƯỜNG SỐ

- KHI GẶP SỰ CỐ, LIÊN HỆ:

+ Trung tâm VNCERT/CC, Cục An toàn thông tin

- qua đầu số tin nhắn **5656**
- hoặc qua website https://chongthurac.vn

+ Trung tâm Giám sát an toàn không gian mạng quốc gia, Cục An toàn thông tin

Địa chỉ trực tuyến tư vấn, hỗ trợ cho người dân tại: https://khonggianmang.vn

Fanpage

Web

Zalo

Sở Thông tin và Truyền thông Quảng Ngãi

https://chuyendoiso.quangngai.gov.vn