



HỘI LIÊN HIỆP PHỤ NỮ TỈNH BÌNH PHƯỚC

SỔ TAY ĐIỆN TỬ

**KIẾN THỨC, KỸ NĂNG ỨNG DỤNG CÔNG NGHỆ THÔNG TIN
VÀ CHUYỂN ĐỔI SỐ**

(Dành cho cán bộ, hội viên, phụ nữ)





HỘI LIÊN HIỆP PHỤ NỮ TỈNH BÌNH PHƯỚC

SỔ TAY ĐIỆN TỬ

THÁNG 4 - NĂM 2025

Ban Thường vụ Hội LHPN tỉnh trân trọng giới thiệu Sổ tay điện tử “Kiến thức, kỹ năng ứng dụng công nghệ thông tin và chuyển đổi số”. Nội dung được trích từ “Tài liệu bồi dưỡng, tập huấn nâng cao năng lực về bảo đảm an toàn thông tin cho đội ngũ nhân lực tuyến cơ sở của các bộ, ngành, địa phương” do Cục an toàn thông tin, Bộ Thông tin và Truyền thông biên soạn, phát hành năm 2024.

“Mỗi cá nhân cần tự trang bị kiến thức và kỹ năng an toàn, an ninh mạng”



ĐẢM BẢO AN TOÀN THÔNG TIN KHI SỬ DỤNG MÁY TÍNH

- 01 Thiết lập mật khẩu an toàn. Cẩn thận với các link, file lạ.
- 02 Kích hoạt chức năng tường lửa.
- 03 Không tải, cài đặt phần mềm không rõ ràng, không cần thiết.
- 04 Cập nhật phần mềm và hệ điều hành.
- 05 Cài đặt phần mềm phòng chống mã độc.
- 06 Mã hóa và sao lưu dữ liệu quan trọng định kỳ, thường xuyên.
- 07 Sử dụng USB, thiết bị lưu trữ di động cẩn trọng.



THIẾT LẬP MẬT KHẨU AN TOÀN

Tấn công mật khẩu là phương pháp tấn công truyền thống và nguy hiểm nhằm vào người dùng.



Sử dụng mật khẩu mạnh



Sử dụng một mật khẩu duy nhất cho từng tài khoản quan trọng như email, tài khoản ngân hàng...



Giữ bí mật mật khẩu bằng cách nhớ hoặc để ở nơi chỉ mình bạn có thể biết và đọc nó



Thiết lập các tùy chọn khôi phục mật khẩu và hãy cập nhật chúng một cách thường xuyên



THIẾT LẬP MẬT KHẨU AN TOÀN

GỢI Ý CÁCH ĐẶT MẬT KHẨU



Mật khẩu ít nhất có 7 ký tự



Sử dụng 4 loại ký tự bao gồm: chữ hoa, chữ thường, chữ số và ký tự đặc biệt (@, #, %...)



Không dùng các mật khẩu dễ đoán, dễ biết như: họ tên, ngày sinh, ngày đặc biệt.



Sử dụng ít nhất 4 ký tự khác nhau và ngẫu nhiên.



Tường lửa hay còn gọi là Firewall giúp bảo vệ hệ thống an toàn cho người dùng, ở đây bạn có thể kiểm tra các kết nối mạng Wifi, kiểm tra và bảo vệ các kết nối hệ thống mạng kịp thời.

LỢI ÍCH

-  Kiểm tra và sửa lỗi mạng Wifi, Internet
-  Báo cáo virus hoặc diệt virus cho máy tính của bạn
-  Giám sát các hoạt động gây bất lợi cho máy tính của bạn
-  Ngăn chặn những vấn đề gây nguy hại cho máy tính
-  Bảo vệ máy tính của bạn khỏi những tác hại khác

**KÍCH HOẠT
CHỨC NĂNG TƯỜNG LỬA**



CÁC BƯỚC CÀI ĐẶT TƯỜNG LỬA

BƯỚC 1

Tại thanh
“Tìm
kiếm”,
nhập và
vào
“Control
Panel”

BƯỚC 2

Chọn
“System
and
Security”

BƯỚC 3

Chọn tiếp
vào
“Windows
Defender
Firewall”

BƯỚC 4

Nhấn chọn
“Turn
Windows
Defender
Firewall on
or off”

BƯỚC 5

Lựa chọn
“Turn on
Windows
Defender
Firewall”

BƯỚC 6

Nhấn OK
để lưu lại
thay đổi

GỠ BỎ CÁC CHƯƠNG TRÌNH KHÔNG CẦN THIẾT

Các thiết bị cá nhân thường được nhà sản xuất cài đặt sẵn các chương trình quảng cáo, giới thiệu hoặc bản dùng thử của các phần mềm khác. Ngoài ra, còn có các chương trình trong quá trình sử dụng được cài đặt. Các chương trình này có thể ẩn chứa các nguy cơ gây mất an toàn thông tin mà kẻ tấn công có thể lợi dụng ngay trong quá trình sử dụng lần đầu tiên hoặc làm giảm hiệu năng của thiết bị.



HƯỚNG DẪN

- 1 Tại thanh “Tìm kiếm”, bạn nhập và vào “Control Panel”
- 2 Tại mục “Programs”, chọn Uninstall a Program
- 3 Tìm đến ứng dụng mà bạn muốn xóa và bấm chuột phải, sau đó chọn Uninstall.

CẬP NHẬT PHẦN MỀM VÀ HỆ ĐIỀU HÀNH

Sau khi cài đặt, hệ điều hành của máy tính hoặc phần mềm có thể là phiên bản cũ chưa được vá lỗi bảo mật. Do đó, người sử dụng cần thiết lập chế độ tự động cập nhật hệ điều hành và các phần mềm khác. Để thực hiện việc này, người dùng mở chức năng Windows Update, sử dụng tùy chọn “Change Settings” để thiết lập việc tự động cập nhật.

HƯỚNG DẪN

1

Mở cửa sổ Start và nhấp vào biểu tượng "răng cưa" Settings (Cài đặt) ở góc dưới bên trái màn hình

2

Trong cửa sổ Settings, chọn Update & Security (Cập nhật & Bảo mật)

3

Cửa sổ Windows Update được mở ra. Nhấn vào nút Check for Updates (Kiểm tra bản cập nhật)

4

Sau khi cập nhật xong, bấm Restart để khởi động lại máy tính

CÀI ĐẶT PHẦN MỀM PHÒNG, CHỐNG MÃ ĐỘC

Phần mềm diệt virus là lớp lá chắn quan trọng bảo vệ người sử dụng khỏi các mã độc và virus. Do đó, cần có chương trình diệt virus để bảo vệ người dùng ngay trong các hoạt động đầu tiên của người sử dụng trên máy tính. Trên thị trường có nhiều hãng cung cấp giải pháp diệt virus, người sử dụng có thể lựa chọn giải pháp miễn phí hoặc các giải pháp thương mại.

HƯỚNG DẪN

- 1 Nhấn Start và chọn Setting
- 2 Chọn Update & Security và chọn Windows Security
- 3 Chọn Open Windows Security

**CÀI ĐẶT PHẦN MỀM
PHÒNG, CHỐNG MÃ ĐỘC**

SỬ DỤNG PHẦN MỀM DIỆT VIRUS CÓ BẢN QUYỀN

Cài đặt phần mềm phòng chống mã độc



MÃ HÓA DỮ LIỆU

Mã hóa là một phương pháp bảo vệ thông tin, bằng cách chuyển đổi thông tin từ dạng có thể đọc và hiểu được thông thường trên các hệ điều hành sang dạng thông tin chỉ có thể đọc được qua giải pháp đã mã hóa.

HƯỚNG DẪN

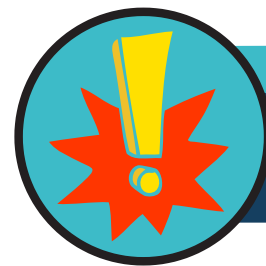
- 1 Nhấp chuột phải lên ổ muốn mã hóa và chọn “Turn on Bitlocker”
- 2 Chọn Use a password to unlock the drive và Nhập mật khẩu bảo vệ
- 3 Chọn lưu Save to a file
- 4 Chọn Encrypt entire drive
- 5 Chọn Compatible mode
- 6 Chọn Start encrypting

MÃ HÓA VÀ SẠO LƯU
DỮ LIỆU

MÃ HÓA VÀ SAO LƯU DỮ LIỆU

SAO LƯU DỮ LIỆU

Bảo vệ dữ liệu quan trọng bằng cách sao lưu chúng vào ổ cứng ngoài hoặc hệ thống lưu trữ trên hạ tầng đám mây. Trường hợp thiết bị của bạn bị nhiễm phần mềm độc hại hoặc bị truy cập bởi hacker, dữ liệu của bạn có thể bị hỏng, bị xóa hoặc mã hóa đòi tiền chuộc ransomware.



LƯU Ý



Đảm bảo thiết bị di động, ổ cứng ngoài sử dụng để sao lưu dữ liệu tách biệt với thiết bị đang sử dụng (không kết nối liên tục qua dây cáp vật lý hoặc mạng cục bộ).

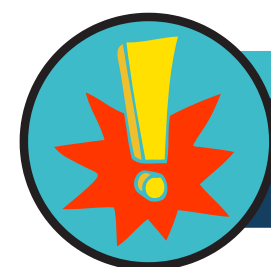


Dịch vụ lưu trữ đám mây rất hữu ích để lưu trữ một bản sao dữ liệu của mình ở nơi khác qua internet.



SỬ DỤNG USB, THIẾT BỊ LƯU TRỮ DI ĐỘNG AN TOÀN

Phần lớn, người dùng đều đã hoặc đang sở hữu thiết bị USB để lưu trữ dữ liệu phục vụ cho việc học tập, làm việc của bản thân. Các thiết bị lưu trữ hoàn toàn có thể bị nhiễm virus và ransomware (vô tình hoặc cố ý) và sử dụng với mục đích xấu, gây thiệt hại cho người sử dụng chúng. Thậm chí còn có những phần mềm độc hại được thiết kế dành riêng cho USB, biến chiếc USB thành công cụ lây nhiễm mã độc trung gian trên máy tính, qua đó đánh cắp thông tin đăng nhập và dữ liệu nhạy cảm.



LƯU Ý

- ✓ Không cắm USB chưa xác định nguồn gốc vào các máy tính quan trọng
- ✓ Luôn dùng giải pháp phòng chống phần mềm độc hại và loại bỏ các mã độc trên các thiết bị lưu trữ di động trước khi sử dụng
- ✓ Không sử dụng chung một ổ USB cho máy tính cả gia đình và cơ quan. Điều này có thể làm giảm nguy cơ lây nhiễm chéo giữa các máy tính
- ✓ Luôn bật các tính năng bảo mật như xác thực mật khẩu, vân tay (nếu có) đối với kết nối USB
- ✓ Luôn cập nhật phần mềm trên máy tính của bạn lên phiên bản mới nhất để được bảo vệ tối đa trước các loại mã độc, lỗ hổng bảo mật đã biết