BỘ THÔNG TIN VÀ TRUYỀN THÔNG

TÀI LIỆU THUYẾT MINH CHUYÊN ĐỀ "KIẾN THỨC, KỸ NĂNG BẢO ĐẢM AN TOÀN KHI SỬ DỤNG MÁY TÍNH VÀ BẢO VỆ DỮ LIỆU"

Hà Nội, năm 2023

1. NHẬN BIẾT CÁC DẤU HIỆU THIẾT BỊ BỊ NHIỄM VIRUS, TẤN CÔNG MẠNG

1. Tổng quan, vai trò

Chúng ta đều biết virus máy tính – và các loại malware khác – có thể gây phiền tóa khiến chúng ta bực mình hoặc nặng nề hơn là gây sự cố an toàn thông tin nghiêm trọng. Một số malware có thể tự sao chép cho tới khi chúng có đầy trên ổ cứng của bạn, biến máy tính của bạn tham gia vào mạng máy tính ma, botnet. Một số loại khác hủy hoại dữ liệu trên máy tính hoặc khiến máy tính hoạt động không ổn định. Một số ít khác thậm chí sử dụng thư điện tử của bạn để phát tán mã độc tới mọi người có trong danh sách bạn bè của bạn. Thậm chí, luôn có những hacker sử dụng malware để chiếm quyền điều khiển máy tính của bạn từ xa, cài mã độc trên máy để tiến hành những vụ tấn công DDOS.

2. Dấu hiệu

Không ai muốn sở hữu một chiếc máy tính bị nhiễm virus. Đó chính là lý do tại sao việc giữ cho máy tính được an toàn là rất quan trọng cũng như cần thiết cài đặt một chương trình diệt virus đáng tin. Bạn có thể tránh được hầu hết các malware chỉ với việc để ý và tránh xa một số bẫy thông thường. Nếu chương trình diệt virus của bạn thường xuyên được cập nhật, nghĩa là bạn đang ở một tình trạng tốt.

Tuy nhiên, một lúc nào đó virus máy tính có thể lọt qua được hệ thống bảo vệ. Có thể do chương trình diệt virus của bạn đã lỗi thời hoặc đã bị xâm nhập bởi một mã độc mới nào đó. Cũng có thể là bạn đã vô tình kích vào đường link đã kích hoạt một loại virus hoặc ai đó đã sử dụng máy tính của bạn để tải một số malware mà bạn không biết.

Làm sao để có thể biết được máy tính của bạn đã bị nhiễm virus? Nếu chương trình diệt virus của bạn thực sự mạnh và được cập nhật đầy đủ, bạn sẽ nhận được thông báo ứng dụng sẽ quét máy tính của bạn và xóa virus đó. Điều này sẽ giúp bảo vệ máy tính của bạn và loại bỏ được virus. Tuy nhiên, nếu phần mềm của bạn bị lỗi thời hoặc virus đã kiểm soát và làm ngưng hoạt động của chương trình diệt virus thì sao? Có dấu hiệu nào cho bạn có thể nhận diện một virus?

Thực chất, có một số dấu hiệu giúp bạn nhận dạng sự hiện diện của malware trong máy tính của mình, hãy cùng tìm hiểu:

a) Máy tính chạy chậm, hoạt động không ổn định

Nếu máy tính của bạn chạy không ổn định, đây là dấu hiệu của máy tính của bạn đã bị mất an toàn thông tin. Một số malware gây rối loạn các file quan trọng giúp máy tính chạy ổn định. Điều này thậm chí còn khiến máy tính của bạn bị hỏng. Nếu máy tính bị hỏng khi bạn cố gắng chạy một ứng dụng nào đó hoặc mở một file cụ thể, sẽ có thông báo rằng dữ liệu của bạn đã bị phá hủy. Chính malware đã gây ra điều này.

b) Cảnh báo giả

Một trong những dấu hiệu gây phiền nhiễu nhất của phần mềm độc hại chính là những cửa sổ pop-up không mong muốn thường xuyên nhảy ra trên máy tính. Nếu việc này xảy ra với tần suất cao thì chắc chắn máy tính của bạn đã dính phần mềm độc hại. Trường hợp này không chỉ gây ảnh hưởng đến việc dùng máy tính mà còn khá khó khăn để loại bỏ chúng khỏi hệ thống. Hơn nữa, chúng còn đi kèm những phần mềm độc hại khác và có thể phá hoại máy tính.

c) Máy tính bị lỗi

Nếu chương trình, hệ thống báo lỗi liên tục hoặc lỗi màn hình xanh xuất hiện thường xuyên thì đó chính là một cảnh báo rõ ràng rằng máy tính đang có vấn đề.

d) Hoạt động đáng ngờ trên ổ cứng:

Nếu nhận thấy ổ đĩa liên tục hoạt động quá mức, ngay cả khi bạn không sử dụng nó, không download hay upload, thì hãy nghĩ đến việc máy tính đã bị nhiễm virus. Tất nhiên, trừ trường hợp ổ cứng của bạn bị lỗi.

đ) Ổ cứng hết dung lượng trống

Bạn cần kiểm tra xem dung lượng lưu trữ vật lý của ổ cứng gần đây có tăng lên hoặc có file nào đã biến mất, bị đổi tên không. Đây là một dấu hiệu hoạt động khác của phần mềm độc hại. Rất nhiều phần mềm độc hại sử dụng những phương pháp khác nhau để "lấp đầy" ổ cứng của bạn và gây ra sự cố trên máy tính nhằm mục đích phá hoại.

e) Phần mềm diệt virus bị tắt

Nếu phần mềm diệt virus dường như không hoạt động hoặc mô-đun cập nhật bị tắt, hãy kiểm tra bảo mật máy tính một cách toàn diện. Một số phần mềm độc hại được thiết kế đặc biệt để vô hiệu hóa các phần mềm diệt virus, khiến bạn không có bất cứ biện pháp phòng tránh nào. Nếu đã cố gắng khởi động lại máy tính, đóng và mở lại phần mềm diệt virus mà vẫn không có tiến triển thì chắc chắn

máy đã bị lây nhiễm phần mềm độc hại. Lúc này có thể phải khởi động lại máy tính ở chế độ Safe Mode và dùng công cụ diệt malware, rootkit chuyên dụng để xử lý.

g) Bạn bè nói rằng họ nhận được thông báo lạ từ bạn

Thông báo lạ này có thể là email, tin nhắn trên các ứng dụng chat. Chúng có thể đính kèm các tập tin hoặc liên kết. Trước hết cần xác định xem những email hoặc tin nhắn đó có phải được gửi từ tài khoản của bạn không. Nếu không có gì bất thường, có thể những thông báo này đã được gửi từ một ứng dụng nằm ngoài sự kiểm soát của bạn.

2. KỸ NĂNG BẢO ĐẢM AN TOÀN THÔNG TIN KHI SỬ DỤNG MÁY TÍNH

Các cách bảo vệ máy tính khỏi các mối đe dọa:

a) Cài đặt phần mềm bảo mật: Trước đây, khả năng bị nhiễm virus khá thấp vì ít người có cơ hội tiếp cận Internet và các phương tiện lưu trữ cũng không đa dạng như bây giờ, nguồn lây nhiễm chính thời đó là trao đổi qua đĩa mềm. Nhưng giờ đây virus phát tán với tốc độ rất nhanh, chỉ trong vòng vài giờ các máy tính tại khắp nơi trên thế giới đều có thể bị đe doạ.

Đảm bảo rằng máy tính được trang bị một phần mềm diệt virus, phần mềm chống malware và tường lửa. Cập nhật và quét máy tính thường xuyên để phát hiện và loại bỏ các mối đe dọa tiềm ẩn.

b) Cập nhật hệ điều hành và phần mềm: Cập nhật Hệ điều hành là việc làm cần thiết. Những kẻ tấn công thường sử dụng sự yếu kém trong bảo mật hệ điều hành để khai thác các điểm yếu. Cập nhật những bản vá quan trọng của hệ điều hành là cách bảo mật, vá các lỗ hổng và bảo đảm an toàn thông tin. Một cách dễ dàng để kiểm tra các bản cập nhật cho Windows là vào Windows Update, nhưng nếu quản lý nhiều máy tính, bạn có thể dùng công cụ mạnh hơn, như MBSA (Microsfoft Baseline Securtity Analyer), công cụ đánh giá điểm yếu miễn phí cho nền tảng Microsoft.

Đảm bảo rằng hệ điều hành và tất cả các chương trình được cài đặt trên máy tính đều được cập nhật mới nhất. Cập nhật này thường chứa các bản vá lỗi và bổ sung tính năng bảo mật mới để ngăn chặn các mối đe dọa.

c) Sử dụng mật khẩu mạnh: Đặt mật khẩu mạnh cho tài khoản người dùng, bao gồm cả mật khẩu đăng nhập vào máy tính và các tài khoản trực tuyến khác.

Sử dụng mật khẩu dài, kết hợp các ký tự chữ cái hoa, chữ cái thường, số và ký tự đặc biệt. Tránh sử dụng mật khẩu dễ đoán như ngày sinh hay tên con vật cưng.

d) Thận trọng khi duyệt web: Tránh truy cập vào các trang web không đáng tin cậy hoặc không an toàn. Cẩn thận với các liên kết không rõ nguồn gốc hoặc email spam có thể chứa mã độc. Sử dụng trình duyệt web đã được cập nhật và bật các cài đặt bảo mật như chặn pop-up và chặn các trang web độc hại.

Không mở tập tin hoặc liên kết không xác định: Tránh mở các tập tin đính kèm hoặc liên kết không xác định trong email hoặc tin nhắn trực tuyến. Điều này có thể là cách các hacker truyền tải mã độc vào máy tính.

đ) Sao lưu dữ liệu thường xuyên: Máy tính an toàn tuyệt đối là khi tắt. Khi bạn bật máy tính, khả năng mất dữ liệu sẽ tăng, thậm chí cả khi bạn không nối với mạng internet. Ổ cứng là một trong những điểm yếu của máy tính và ổ cứng hỏng là một khả năng có thể xảy ra. Hoặc bạn có thể vô tình xoá mất file dữ liệu. Vì thế, chúng ta cần sao lưu dữ liệu, dùng CD, DVD, ổ cứng hay trên các phương tiện lưu trữ khác.đảm bảo sao lưu dữ liệu quan trọng thường xuyên, sử dụng các thiết bị lưu trữ ngoài hoặc dịch vụ đám mây. Điều này giúp phục hồi dữ liệu trong trường hợp bị tấn công hoặc mất dữ liệu.

e) Hạn chế quyền truy cập: Cân nhắc hạn chế quyền truy cập vào máy tính . Sử dụng tài khoản người dùng có đặc quyền hạn chế cho các hoạt động hàng ngày và tránh sử dụng tài khoản quản trị viên khi không cần thiết.

g) Sử dụng kết nối mạng an toàn: Khi kết nối đến mạng Wi-Fi công cộng, sử dụng kết nối VPN để mã hóa dữ liệu và bảo mật thông tin.

h) Giám sát tài khoản và giao dịch trực tuyến: Theo dõi tài khoản ngân hàng và các giao dịch trực tuyến một cách cẩn thận. Báo cáo ngay lập tức bất kỳ hoạt động không xác định hoặc nghi ngờ đến dịch vụ cung cấp tài khoản.

i) Đào tạo và nhận thức an ninh: Tăng cường kiến thức về an ninh mạng và cung cấp sự nhận thức về các mối đe dọa mới nhất. Tham gia các khóa học, đọc sách và tài liệu liên quan để trang bị bản thân với kiến thức cần thiết.

3. THIẾT LẬP, SỬ DỤNG USB VÀ THIẾT BỊ LƯU TRỮ AN TOÀN

3.1. Chọn USB và thiết bị lưu trữ đáng tin cậy

Thương hiệu và nhà sản xuất: Chọn USB và thiết bị lưu trữ từ các thương hiệu và nhà sản xuất uy tín, có tiếng trong ngành công nghệ thông tin. Các nhà sản xuất đã được công nhận thường tuân thủ các tiêu chuẩn chất lượng và an toàn.

Đánh giá và đánh giá của người dùng: Trao đổi với cộng đồng người dùng và đọc các đánh giá, đánh giá về sản phẩm trước khi mua. Điều này giúp có cái nhìn tổng quan về độ tin cậy và hiệu suất của USB và thiết bị lưu trữ mà đang quan tâm.

Dung lượng và tốc độ truyền dữ liệu: Xác định dung lượng lưu trữ cần thiết cho nhu cầu và chọn USB hoặc thiết bị lưu trữ có dung lượng phù hợp. Ngoài ra, kiểm tra tốc độ truyền dữ liệu để đảm bảo rằng nó đáp ứng được yêu cầu .

Tiêu chuẩn bảo vệ dữ liệu: Hãy tìm hiểu về các tiêu chuẩn bảo vệ dữ liệu mà USB và thiết bị lưu trữ hỗ trợ, chẳng hạn như mã hóa phần cứng hay chứng nhận bảo mật. Điều này giúp đảm bảo rằng dữ liệu được bảo vệ một cách an toàn trên thiết bị.

Hỗ trợ khách hàng và bảo hành: Kiểm tra chính sách hỗ trợ khách hàng và bảo hành của nhà sản xuất để đảm bảo rằng sẽ nhận được sự hỗ trợ và bảo vệ phù hợp trong trường hợp có sự cố với USB hoặc thiết bị lưu trữ.

3.2. Sử dụng phần mềm diệt virus và quét thiết bị

Cài đặt phần mềm diệt virus đáng tin cậy: Chọn một phần mềm diệt virus từ các nhà cung cấp uy tín và có tiếng trong ngành. Đảm bảo cập nhật phiên bản mới nhất của phần mềm để nắm bắt các mối đe dọa mới nhất.

Quét toàn bộ thiết bị: Trước khi sử dụng USB hoặc thiết bị lưu trữ mới, hãy thực hiện một quét toàn bộ để phát hiện và loại bỏ bất kỳ phần mềm độc hại nào có thể tồn tại trên thiết bị. Chế độ quét toàn bộ sẽ kiểm tra tất cả các tệp và thư mục trên thiết bị.

Quét định kỳ: Thực hiện quét định kỳ cho USB và thiết bị lưu trữ đã sử dụng để đảm bảo rằng chúng không bị nhiễm virus hay phần mềm độc hại. Quét định kỳ giúp phát hiện các mối đe dọa mới và ngăn chặn sự lây lan của chúng.

Cập nhật định kỳ: Đảm bảo rằng phần mềm diệt virus và cơ sở dữ liệu đang được cập nhật định kỳ. Nhà cung cấp phần mềm thường cung cấp các bản vá và cập nhật mới để chống lại các mối đe dọa mới. Việc cập nhật định kỳ đảm bảo rằng có các công nghệ bảo mật mới nhất.

Chế độ quét thích hợp: Thay đổi chế độ quét tùy thuộc vào nhu cầu và tính năng của thiết bị. Ví dụ, có thể chọn quét nhanh khi cần quét nhanh chóng hoặc quét chi tiết khi cần kiểm tra toàn bộ hệ thống.

Phản ứng với các cảnh báo: Nếu phần mềm diệt virus phát hiện một tệp hoặc thiết bị bị nhiễm virus, hãy tuân thủ các hướng dẫn của phần mềm để xử lý tình huống. Đừng bỏ qua cảnh báo hoặc bỏ qua các biện pháp bảo vệ.

3.3. Mã hóa dữ liệu khi sử dụng USB và thiết bị lưu trữ

Sử dụng phần mềm mã hóa: Cài đặt một phần mềm mã hóa dữ liệu trên máy tính để mã hóa các tệp tin và thư mục trước khi sao chép vào USB hoặc thiết bị lưu trữ. Có nhiều phần mềm mã hóa mạnh mẽ và dễ sử dụng có sẵn để lựa chọn.

Mã hóa toàn bộ USB hoặc thiết bị lưu trữ: Nếu muốn bảo vệ toàn bộ nội dung của USB hoặc thiết bị lưu trữ, hãy xem xét sử dụng tính năng mã hóa được tích hợp sẵn trong hệ điều hành hoặc phần mềm mã hóa bên thứ ba để mã hóa toàn bộ ổ đĩa hoặc phân vùng của thiết bị.

Tạo một phân vùng mã hóa riêng: Nếu chỉ muốn mã hóa một phần của USB hoặc thiết bị lưu trữ, có thể tạo một phân vùng mã hóa riêng trên thiết bị. Điều này cho phép lưu trữ dữ liệu mã hóa và dữ liệu không mã hóa trên cùng một thiết bị.

Thực hiện kiểm tra và cập nhật định kỳ: Kiểm tra và cập nhật phần mềm mã hóa thường xuyên để đảm bảo rằng sử dụng phiên bản mới nhất và hạn chế các lỗ hổng bảo mật

3.4. Hạn chế chia sẻ USB và thiết bị lưu trữ

Sử dụng USB và thiết bị lưu trữ riêng: Sử dụng USB và thiết bị lưu trữ riêng và không chia sẻ chúng với người khác. Điều này giảm khả năng tiếp xúc với phần mềm độc hại từ nguồn khác.

Hạn chế kết nối USB với các máy tính không đáng tin cậy: Tránh kết nối USB với các máy tính không đáng tin cậy hoặc không rõ nguồn gốc. Máy tính không an toàn có thể chứa phần mềm độc hại hoặc virus có thể lây lan vào USB

Không chia sẻ dữ liệu nhạy cảm: Tránh chia sẻ dữ liệu nhạy cảm hoặc quan trọng trên USB hoặc thiết bị lưu trữ. Nếu cần, hãy mã hóa dữ liệu trước khi chia sẻ để đảm bảo rằng chỉ có những người cần thiết mới có thể truy cập.

4. BẢO VỆ, SAO LƯU, PHỤC HỒI DỮ LIỆU

4.1. Bảo vệ dữ liệu

Một website sẽ chứa đựng rất nhiều loại thông tin. Tuy nhiên, không phải thông tin nào cũng cần được bảo vệ. Vì thế, trước tiên, bạn cần xác định được dữ liệu nào là quan trọng đối cá nhân và công việc của mình để tiến hành mã hóa bảo vệ chúng.

Các phương pháp bảo vệ dữ liệu

Sử dụng hệ thống phần mềm antivirus và chống spyware chất lượng

Antivirus là phần mềm giữ cho hệ thống và dữ liệu của bạn an toàn khỏi virus máy tính và các cuộc tấn công phần mềm độc hại. Ngoài ra, chúng có thể phát hiện và xóa những phần mềm độc hại ra khỏi hệ thống và dữ liệu của bạn.

Trong khi đó, Spyware là một loại phần mềm độc hại, lấy cắp các thông tin người dùng như mật khẩu, thông tin thẻ thanh toán,… Spyware thường tấn công thông qua các liên kết lạ hoặc chấp nhận các điều khoản dịch vụ khi tải xuống một phần mềm mà không đọc rõ thông tin,…

Bật tường lửa

Hầu hết các hệ thống máy tính đều có tường lửa tích hợp sẵn trong hệ điều hành giúp bảo mật web. Việc bạn cần làm chỉ là đảm bảo bật tường lửa trước khi thêm các thiết bị mới như modem, máy in hoặc bất kỳ thiết bị được kết nối nào vào mạng máy tính.

Sử dụng mật khẩu mạnh

Mật khẩu mạnh là yếu tố quan trọng đầu tiên bạn cần lưu ý. Bạn không nên sử dụng các mật khẩu dễ đoán. Bên cạnh đó, bạn cũng nên lưu ý không đặt mật khẩu giống nhau cho tài khoản trên nhiều nền tảng, tránh trường hợp các thông tin liên quan đều bị xâm phạm khi một mật khẩu bị đánh cắp.

Sao lưu dữ liệu

Sao lưu dữ liệu là bước quan trọng giúp chúng ta dễ dàng khôi phục lại những thông tin và dữ liệu một khi chúng bị đánh cắp và nhanh chóng quay về trạng thái hoạt động bình thường. Bạn có thể thực hiện sao lưu trên các nền tảng điện toán đám mây hoặc trung tâm dữ liệu.

Mã hóa dữ liệu

Thực hiện chuyển đổi dữ liệu quan trọng sang một ngôn ngữ đã được mã hóa, và những dữ liệu này chỉ có thể được mở bằng mật khẩu. Tuy nhiên, bảo vệ

dữ liệu theo cách này có thể gây ra vấn đề phát sinh nếu cá nhân sử dụng thiết bị riêng, ổ đĩa ngoài cũng như các ứng dụng không thuộc phạm vi quản lý.

4.2. Sao lưu dữ liệu

Sao lưu dữ liệu là bản sao của dữ liệu hệ thống, cấu hình hoặc ứng dụng của bạn được lưu trữ riêng biệt với bản gốc. Đôi khi các tổ chức có thể gặp phải các sự kiện không mong muốn như thiên tai, lỗi con người, sự kiện bảo mật hoặc lỗi hệ thống. Sao lưu dữ liệu là một chức năng bảo vệ dữ liệu quan trọng để giảm nguy cơ mất dữ liệu toàn bộ hoặc một phần trong trường hợp xảy ra các sự kiện không mong muốn. Nó cung cấp cho các tổ chức khả năng khôi phục các hệ thống và ứng dụng về trạng thái mong muốn trước đó.

4.3. Hướng dẫn mã hóa dữ liệu

Mã hóa dữ liệu là quá trình chuyển đổi thông tin từ dạng ban đầu thành dạng mã hóa, mà chỉ có thể được giải mã và đọc bởi những người có chìa khóa mã hóa tương ứng. Mục đích của mã hóa dữ liệu là bảo vệ thông tin quan trọng khỏi sự truy cập trái phép và lộ thông tin khi dữ liệu được lưu trữ, truyền tải hoặc chia sẻ.

Hôm nay, tôi sẽ giới thiệu cho các bạn phương pháp mã hóa đơn giản bằng cách sử dụng dịch vụ lưu trữ đám mây của Google Drive và Dropbox

a) Google Drive

Tất cả các tệp được tải lên Drive hoặc được tạo trong Docs đều được mã hóa khi chuyển tiếp với mã hóa AES 256 bit. Để tăng tính bảo mật, tổ chức của bạn có thể cho phép bạn mã hóa tệp trong Google Drive, Docs, Sheets, Slides bằng mã hóa phía máy khách của Google Workspace. Các tệp được mã hóa có một số hạn chế so với các tệp tiêu chuẩn. Người dùng cũng có thể tải lên bất kỳ loại tệp Drive nào như PDF và .docx dưới dạng tệp Drive được mã hóa và tạo Docs, Sheets, Slides được mã hóa.

Điều khác biệt về các tệp được mã hóa

Bạn có thể nhận ra mọi tệp được mã hóa trong Drive thông qua khóa.

Chỉ một người dùng có thể chỉnh sửa một tệp được mã hóa vào một thời điểm.

Tự động lưu hoạt động khác nhau đối với các tệp được mã hóa. Tự động lưu bắt đầu cứ sau 5 phút, trừ khi thiết bị không hoạt động hoặc bạn đang thực

hiện một hành động khác, chẳng hạn như bạn chia sẻ tệp hoặc cố gắng thoát khỏi tệp.

(Nếu bạn cố gắng thoát ra khỏi tệp chưa được lưu, bạn sẽ nhận được một cảnh báo. Để tránh mất những thay đổi chưa lưu, hãy nhấp vào HỦY).

Tự động lưu có 3 trạng thái:

- Đang chờ lưu: đang chờ kích hoạt lưu tự động hoặc bộ hẹn giờ 5 phút.

- Đang lưu: đang lưu, bạn có thể tiếp tục chỉnh sửa tệp của mình

- Đã lưu vào Drive: bạn chưa thực hiện bất kỳ thay đổi nào

Có các bước khác nhau để tạo tệp được mã hóa.

Admin có thể yêu cầu người dùng đăng nhập vào một dịch vụ SSO bổ sung để truy cập các tệp được mã hóa. Nghĩa là người dùng có thể phải đăng nhập hai lần: một lần cho IDP của tổ chức của bạn và một lần với Google cho Drive, Docs, Sheets, Slides.

Người dùng có thể in từ Docs xuống nhưng không in được trong Sheets và Slides.

(beta) Có thể xuất tệp Google Sheets thành tệp Excel > Đi tới Tải xuống tệp.

Lịch sử phiên bản cho các tệp được mã hóa giữ lại tối đa 100 phiên bản. Sau khi bạn vượt quá 100 phiên bản, các phiên bản ít quan trọng hơn sẽ tự động bị xóa.

Docs, Sheets, Slides được mã hóa có kích thước tối đa là 100MB.

Số lượng ảnh tối đa trong một tài liệu: 3000 ảnh.

Kích thước một hình ảnh là 1MB.

Tính năng không có sẵn cho các tệp được mã hóa

Với các tệp mã hóa, người dùng không thể:

- Truy cập chế độ chỉnh sửa Office

- Bình luận

- Sử dụng ứng dụng dành cho thiết bị di động để chỉnh sửa Docs, Sheets, Slides.

- Sử dụng các chức năng trong Sheets để thực hiện cuộc gọi bên ngoài.

- Mở tệp Microsoft Office bằng Docs, Sheets, Slides.

- Sử dụng một số công cụ nhất định, bao gồm: kiểm tra chính tả, kiểm tra ngữ pháp, dịch và so sánh tài liệu, nhập liệu bằng giọng nói và tiện ích bổ sung.

- Sử dụng bản xem trước tệp cho các tệp trên Drive (không phải tệp Docs, Sheets, Slides)

- Truy cập tệp được mã hóa ngoại tuyến.

Tạo hoặc sao chép các tệp được mã hóa

Để tạo một tài liệu, bảng tính hoặc bản trình bày được mã hóa mới, hãy chọn một tùy chọn:

- Từ Google Drive:

+ Truy cập drive.google.com

+ Ở trên cùng bên trái, nhấp vào New (Mới)

+ Di chuột qua mũi tên bên cạnh Docs, Sheets, Slides > Blank encrypted document/spreadsheet/presentation (Tài liệu/Bảng tính/Bản trình bày được mã hóa trống) > Create (Tạo)

- Từ Google Docs, Sheets, Slides:

+ Mở Google Docs, Sheets, Slides > File

+ New (Mới) > New encrypted document/spreadsheet/presentation (Tạo tài liệu/bảng tính/bản trình bày mới) > Create (Tạo)

- Để tải lên một tệp được mã hóa mới:

+ Truy cập drive.google.com

+ Ở trên cùng bên trái, nhấp vào New (Mới) > Encrypt and upload file (Tải lên file mã hóa)

Để sao chép một tệp được mã hóa, hãy nhấp chuột phải hoặc nhấp đúp vào tệp, sau đó chọn Make a copy (Tạo bản sao). Người dùng cũng có thể chọn Make a encrypted copy (Tạo bảo sao được mã hóa) nếu tệp chưa có mã hóa cũng như tạo Make a decrypted copy (Tạo bản sao được giải mã).

Lưu ý: tính năng này hiện chỉ khả dụng cho các tệp Drive (không phải Docs, Sheets, Slides)

b) Dropbox

Dropbox được biến đến là một trong những dịch vụ lưu trữ trực tuyến đám mây phổ biến nhất hiện nay, tuy được rất nhiều người sử dụng nhưng có lẽ Dropbox vẫn chưa thực sự quan tâm đến người dùng khi các file được up lên hệ thống này chỉ có một lớp bảo mật chung duy nhất mà thôi

Bước 1: Bạn cần tải phần mềm giúp bạn mã hóa file Dropbox là BoxCryptor.

Bước 2: Tiến hành cài đặt thông thường, lưu ý đóng tất cả các trình duyệt lại khi cài phần mềm này nhé và khi có thông báo yêu cầu bảo mật từ hệ thống, bạn bấm tiếp vào install

Bước 3: Sau khi cài đặt xong bạn bấm vào Create your Boxcrytor account để tiến hành tạo tài khoản nếu chưa có.

Bước 4: Điền đầy đủ các thông số tương tự như trong hình và kết thúc quá trình tạo tài khoản bằng Next .

Bước 5: Click chọn i understand that it is my own responsibility to remember my password rồi ấn Next.

Bước 6: Click tiếp Free để sử dụng, chúng ta chỉ cần mức Free cũng đủ bảo vệ dữ liệu Dropbox.

Bước 7: Sau khi đăng ký tài khoản hoàn tất, tiến hành đăng nhập với các thông tin đã có sẵn nhé.

Bước 8: Khi đăng nhập thành công, phần mềm sẽ yêu cầu bạn chọn thư mục để mã hóa , bạn có thể thêm hoặc remove sau thoải mái nên bạn cứ tùy chọn lấy một folder mình cần.

Bước 9: Ngay lập tức phần mềm sẽ hiện thông báo bạn đã thêm thành công khu vực cần mã hóa.

Bước 10: Lúc này BoxCrytor sẽ tạo ra 1 ổ riêng và bạn có thể truy cập được vào.

Bước 11: Để mã hóa ta chọn 1 file trong ổ được chỉ định, click bọn Boxcrytor >Encrypt .

Bước 12: Ngay lúc này bạn quay trở ra khu vực được chỉ định mã hóa, bạn sẽ thấy file của bạn được mã hóa khác biệt với các file còn lại.

Bước 13: Và khi share lên Dropbox cũng vậy, mã hóa sẽ được gỡ ra chỉ với 2 tiêu chí duy nhất là bạn hoặc người được bạn chỉ định nhận file này (người nhận cũng phải có BoxCrytor).

4.4. Hướng dẫn sao lưu dữ liệu định kì

Sao lưu dữ liệu định kỳ là một biện pháp quan trọng để đảm bảo an toàn và khôi phục dữ liệu trong trường hợp mất mát, hỏng hóc hoặc tình huống khẩn cấp. Dưới đây là một số hướng dẫn để thực hiện sao lưu dữ liệu định kỳ bằng cách sử dụng Google Drive để lưu trữ dữ liệu và sao lưu dữ liệu một cách đơn giản.

Google Drive là dịch vụ lưu trữ dữ liệu trực tuyến phổ biến của Google. Với tính năng bảo mật cao, lưu trữ dữ liệu vô thời hạn. Tuy nhiên, nhiều người lại chưa biết cách thực hiện và sử dụng dịch vụ này. Chuyên đề này sẽ hướng dẫn bạn tạo và sử dụng Google Drive để lưu trữ dữ liệu hiệu quả.

a) Tạo tài khoản

- Truy cập Google Drive > Chọn Truy cập Google Drive.

- Bấm Tạo tài khoản rồi chọn Cho bản thân tôi.

- Điền đầy đủ các thông tin yêu cầu, sau đó chọn Tiếp theo.

- Nhập mã xác minh mà Google gửi cho bạn thông qua số điện thoại vừa nhập > Chọn Xác minh.

- Chấp nhận các điều khoản của Google bằng cách chọn Tôi đồng ý.

b) Hướng dẫn sử dụng Google Drive trên máy tính

- Vào thư mục bạn muốn tải lên dữ liệu, chọn Mới.

- Chọn tải tệp hoặc thư mục.

- Chọn tập tin, thư mục bạn muốn tải lên và chọn Open.

- Chờ việc tải lên hoàn tất. Lưu ý không được tắt trang Google Drive trong quá trình tải.

c) Hướng dẫn sử dụng Google Drive trên điện thoại

- Mở ứng dụng Google Drive và tiến hành đăng nhập tài khoản.

- Chọn biểu tượng dấu cộng (+) ở góc phải bên dưới màn hình.

- Chọn công cụ để tải lên.

- Chọn tệp, thư mục muốn tải lên Google Drive và đợi hoàn tất..

5. ĐIỆN TOÁN ĐÁM MÂY

5.1. Điện toán đám mây là gì?

Điện toán đám mây (Cloud Computing) hay còn gọi là điện toán máy chủ ảo cung cấp các công nghệ, tài nguyên máy tính liên kết với mạng Internet. Với mô hình điện toán đám mây, người dùng sẽ được tiếp cận các tài nguyên từ công nghệ, năng lượng điện toán, lưu trữ cơ sở dữ liệu đến từ những nhà cung cấp dịch vụ đám mây.

Nếu như đang sử dụng những ứng dụng web từ các hãng lớn như Google hoặc Microsoft thì chính bạn đang sử dụng Cloud Computing. Các ứng dụng web như Gmail, Google Calender, Hotmail, SaleForce, Dropbox và Google Docs đều dựa trên Cloud Computing bởi vì khi kết nối tới những dịch vụ đó, người dùng đã được truy cập vào những cụm nhóm máy chủ đồ sộ thống nhất trên Internet.

5.2. Lợi ích của điện toán đám mây

Điện toán đám mây mang lại rất nhiều lợi ích giúp cho doanh nghiệp tối ưu lại tài nguyên và nhân lực như:

- Tiết kiệm chi phí: Doanh nghiệp chỉ cần trả tiền cho những dịch vụ mà mình sử dụng mà không cần phải bỏ ra các khoản như phí mua thiết bị lắp đặt hệ thống, phí vận hành và duy trì như các máy chủ vật lý hay VPS.

- Sử dụng linh hoạt và dễ mở rộng cơ sở hạ tầng: Người dùng có thể thay đổi tăng hoặc giảm bớt tài nguyên phù hợp với nhu cầu sử dụng của mình.

- Truy cập và sử dụng ở bất cứ mọi nơi: Người dùng có thể truy cập và sử dụng điện toán đám mây ở bất kỳ nơi nào trên thế giới qua internet.

- Tính sẵn sàng cao: Hệ thống điện toán đám mây luôn có cơ chế dự phòng sau lưu dữ liệu nên người dùng có thể nhanh chóng khôi phục dữ liệu khi gặp sự cố trong quá trình sử dụng.

- Độ bảo mật và an toàn cao: Các nhà cung cấp điện toán đám mây sẽ có những trung tâm dữ liệu lớn, hệ thống bảo mật nhiều tầng nên độ an toàn sẽ tốt hơn nhiều so các doanh nghiệp không chuyên về công nghệ.

5.3. Tại sao nên dùng điện toán đám mây

Theo cách truyền thống, những công ty lớn, những tập đoàn lớn thường cài đặt tất cả các ứng dụng hay phần mềm trên những cụm máy chủ của họ. Nếu một công ty sẽ có một hệ thống máy chủ, 2 công ty sẽ là 2, và 1000 công ty sẽ sở hữu

con số máy chủ tương ứng. Bởi vậy, để giảm tải các chi phí phát sinh từ hệ thống máy chủ đồ sộ của các công ty riêng lẻ, Điện toán đám mây đã được ra đời. Và như đã nói ở trên, ”đám mây” chính là dùng để chỉ Internet, một mạng lưới gần như vô tận.

Hiện tại đã có rất nhiều doanh nghiệp đăng tải ứng dụng của họ lên Internet và được thêm thắt rất nhiều tính năng mới thông qua trình duyệt web. Một bằng chứng gần đây nhất chính là sự xuất hiện của Chrome OS, một hệ điều hành với giao diện và ứng dụng đầy đủ ngay trên trình duyệt web. Sớm hay muộn, bạn sẽ có thể kết nối tới bất cứ ứng dụng nào chỉ với việc thông qua trình duyệt web trên PC.

5.4. An toàn khi sử dụng Nền tảng điện toán đám mây

Bên cạnh những lợi tính năng ưu việt và lợi ích to lớn, còn có những nhược điểm của các hình thức lưu trữ đám mây mà người dùng cần lưu tâm để đảm bảo sự an toàn và bảo mật dữ liệu trên Internet.

a) Hiểu rõ nhu cầu

Các dịch vụ lưu trữ đám mây đều có 1 vấn đề chung giống các xu hướng mới khác đó là 1 bộ phận không nhỏ người đùng đều chạy theo xu hướng, phong trào trong khi chưa hiểu biết đầy đủ về những gì đang sử dụng, tham gia.

Hãy tìm hiểu kỹ càng các tính năng và những gì điện toán đám mây có thể đem lại cho bạn trước khi bắt đầu sử dụng đến điện toán đám mây. Đơn thuần điện toán đám mây chỉ là 1 công cụ đáp ứng những nhu cầu nhất định. Đừng sử dụng nó chỉ để chứng tỏ mình bắt kịp công nghệ, bạn sẽ làm lãng phí nó.

b) Lựa chọn đúng dịch vụ đám mây

Hiện nay có rất nhiều dịch vụ đám mây nổi tiếng rất phổ biến và đều hỗ trợ người dùng tương đối tốt như Dropbox, Skydrive, Box, Google Drive, Amazon Cloud Drive....Trước khi quyết định sử dụng dịch vụ nào, hãy xem xét và tìm hiểu tất cả các lựa chọn.

Bạn có thể so sánh các dịch vụ thông qua sự tiện lợi, tiết kiệm thời gian, công sức của bạn. Vì điện toán đám mây về bản chất là dữ liệu di chuyển giữa các đám mây nên có thể tiêu tốn khá nhiều thời gian. Nếu dịch vụ nào cung cấp các tính năng tạo ổ đĩa , thư mục trên máy tính, ứng dụng desktop thì sẽ tiện lợi hơn rất nhiều so với việc tải và download dữ liệu từ web. Ngoài ra vấn đề đồng bộ dữ liệu cũng là vấn đề đáng lưu tâm. Hãy chắc chắn rằng bạn có thể truy cập và sử

dụng dữ liệu đám mây của bạn ở bất cứ nơi đâu, với bất kỳ thiết bị nào có kết nối Internet.

c) Tạo nhiều bản sao của dữ liệu

Một lời khuyên là đừng bao giờ sử dụng lưu trữ đám mây như 1 kho lưu trữ dữ liệu duy nhất. Bởi một trong những rủi ro lớn của các dịch vụ điện toán đám mây là tuổi thọ của chúng nằm ngoài tầm kiểm soát của bạn. Nó có thể biến mất ngay ngày mai mà không báo trước, kèm theo đó là sự mất mát về dữ liệu của bạn. Vì vậy hãy coi dữ liệu trên đám mây chỉ là một bản sao lưu. Do vậy sử dụng các phương thức sao lưu song song với việc lưu trữ đám mây là sự lựa chọn cần thiết dành cho bạn.

d) Bảo vệ dữ liệu

Như phần trên đã đề cập đến vấn đề an toàn dữ liệu và đề phòng bảo vệ, sao lưu dữ liệu khi nhà cung cấp bị sập. Tuy nhiên ngoài vấn đề đó, vấn đề về bảo mật dữ liệu cũng thật sự cần được lưu tâm. Nếu nhà cung cấp dịch vụ bị hack, dữ liệu của bạn thật sự sẽ bị lâm nguy bởi hacker sẽ nắm toàn quyền truy cập vào dữ liệu của bạn. Hãy sử dụng các ứng dụng mã hóa để bảo mật cho đám mây của bạn. Một số lựa chọn tốt đó là các ứng dụng TrueCrypt, BoxCryptor, TeamDrive, SpiderOak...hoặc dùng mã nguồn mở EncFS nếu máy tính của bạn đang chạy hệ điều hành Linux./.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG