Microsoft MOET ICTD VIETNET-ICT

CHƯƠNG TRÌNH TIN HỌC ỨNG DỤNG VÀ KHOA HỌC MÁY TÍNH

CẨM NANG AN TOÀN SỬ DỤNG INTERNET

Dành cho học sinh và phụ huynh

DỰ ÁN TĂNG CƯỜNG KỸ NĂNG CÔNG NGHỆ THÔNG TIN
CHO GIỚI TRẺ HỘI NHẬP VÀ PHÁT TRIỂN

PHẦN I:
DÀNH CHO HỌC SINH

I. Tại sao cần đảm bảo an toàn sử dụng Internet

Việt Nam có mức độ sử dụng Internet tăng trưởng cao, từ gần 3,1 triệu người dùng năm 2003 đến 45,5 triệu người dùng năm 2015 tương đương 48% dân số, 146% dân số sử dụng thuê bao di động và 31% sử dụng mạng xã hội. Việt Nam đang được xếp thứ 6 trong khu vực châu Á về số lượng người dùng và đứng thứ 17/20 quốc gia có lượng người dùng Internet nhiều nhất thế giới , một nửa trong số đó là trẻ em và thanh thiếu niên (1). Chúng ta ngày càng không thể phủ nhận được công nghệ, thiết bị số và Internet đóng một vai trò quan trọng trong cuộc sống thường ngày, phục vụ giải trí, làm việc, học tập và kết nối. Tuy nhiên, mặt trái của Internet và công nghệ di động là mang lại nhiều thách thức đối với an toàn của người dùng, đặc biệt là trẻ em.

(1) Theo Tổ chức thống kê số liệu Internet quốc tế (internetworldstats), 2015

Uy tín và hình ảnh cá nhân

Tất cả những gì bạn đăng tải trên môi trường trực tuyến đều trở thành một phần uy tín và hình ảnh cá nhân của bạn.

Internet tồn tại lâu dài, rộng khắp và thông tin trực tuyến luôn luôn có thể tìm kiếm và theo dõi một cách dễ dàng. Vì vậy, bất kể một thông tin nào chúng ta đã đăng tải lên cũng có thể được tìm ra bởi nhà tuyển dụng trong tương lai.

Mối quan hệ

Cũng như trong đời sống thực tế, những mối quan hệ trong môi trường trực tuyến cũng rất phức tạp. Chúng ta có thể có những cuộc tranh luận thậm chí với cả người thân thông qua việc nhắn tin, có thể tạo một cộng đồng trực tuyến và cũng có thể tìm ra những người bạn thông qua mạng xã hội.

Bảo mật cá nhân

Bạn có thể bị đánh cắp thông tin cá nhân hoặc quyền bảo mật trên môi trường trực tuyến, kẻ xấu có thể lấy cắp thông tin bạn chia sẻ thông qua những hình ảnh, video, dòng trạng thái bạn đăng tải trên mạng xã hội và bất cứ đâu trên Internet.

Tài chính

Những người trẻ chính là những người có nguy cơ bị xâm phạm tài chính nhiều nhất trên môi trường trực tuyến. Những kẻ trộm thường nhắm vào những bạn trẻ vì họ có tài chính tốt và lơ là trong việc bảo mật thông tin cá nhân. Kẻ xấu cũng thường có những hành vi lừa đảo tinh vi như thành lập các trang web rồi yêu cầu

người dùng đăng ký thông tin cá nhân hoặc gửi email yêu cầu bạn đi theo một đường dẫn tới các trang web để cập nhật và xác nhận tên tài khoản, mật khẩu.

Tại Việt Nam, hiện có rất ít thông tin và dữ liệu về mức độ và quy mô của xâm hại và bóc lột trẻ em qua môi trường trực tuyến. 14% thanh thiếu niên được hỏi ở khu vực thành thị và 20% thanh thiếu niên được hỏi ở khu vực nông thôn cho biết họ đã từng trải nghiệm việc bị bắt nạt trong môi trường kỹ thuật số như bắt nạt qua mạng, đe dọa hoặc gây bối rối khó xử (2).

Năm 2014, Bộ Lao Động, Thương Binh và Xã Hội tiến hành khảo sát với học sinh 3 trường trung học phổ thông tại Hà Nội trong đó 36.4% đã từng bị bắt nạt;15.7% đã từng bị đe dọa và 13.2% bị gây khó xử. Trung tâm Sáng kiến Sức khỏe và Dân số (CCIHP) và Bộ Lao Động, Thương Binh và Xã Hội tiến hành khảo sát với 246 thanh thiếu niên trong năm 2014 thì bắt nạt, nhắn tin gạ tình và tiếp cận hình ảnh khiêu dâm không mong muốn là các vấn đề thanh thiếu niên gặp phải nhiều nhất, chủ yếu qua mạng xã hội (3).

Vì vậy, điều quan trọng nhất hiện nay, bên cạnh việc các đơn vị cung cấp dịch vụ trực tuyến cần có trách nhiệm trong hỗ trợ bảo vệ trẻ em và thanh thiếu niên – những người dùng dịch vụ của họ thông qua việc thiết lập các cơ chế để sử dụng dịch vụ một cách an toàn hơn, thông qua bảo vệ danh tính và dữ liệu cá nhân, đảm bảo quyền tự do biểu đạt của trẻ em và thiết lập các cơ chế để giải quyết các vi phạm về quyền trẻ em khi xảy ra; thì chính trẻ em và các bậc phụ huynh cần tự trang bị cho mình những kỹ năng cần thiết để bảo vệ chính mình và người thân khỏi những nguy cơ gây hại trên môi trường trực tuyến.

(2) UNICEF New York, Vụ Truyền Thông, Phòng Truyền thông Xã hội và Dân sự : Thanh thiếu niên Việt Nam trực tuyến: thử nghiên cứu về bức tranh kỹ thuật số Việt Nam, 2013
(3) Sơ lược về bảo vệ trẻ em trên môi trường trực tuyến, UNICEF, 2015

II. Làm thế nào để đảm bảo an toàn trên môi trường trực tuyến

1. Bảo vệ các thiết bị kết nối Internet (máy tính, điện thoại)

- Tăng cường tính phòng thủ cho máy tính

Hãy để chế độ tự động cập nhật cho tất cả các phần mềm (bao gồm cả trình duyệt web) trên máy tính của bạn.

Cài đặt phần mềm diệt virus và phần mềm chống gián điệp.

Luôn luôn bật tường lửa (firewall): Tường lửa giúp tạo nên một hàng rào bảo vệ máy tính của bạn trước những nguy hại từ môi trường Internet. Chỉ cần bạn tắt tường lửa đi trong một vài phút cũng có thể làm gia tăng nguy cơ máy tính của bạn bị xâm hại bởi những mối nguy hiểm trực tuyến.

Cẩn trọng khi sử dụng ổ flash (ổ cứng di động sử dụng cổng USB để kết nối). Ổ cứng di động hoặc USB có thể mang virus gây hại cho máy tính, vì vậy hãy cẩn trọng mỗi khi kết nối ổ cứng hoặc USB với máy tính của bạn: Không sử dụng ổ cứng hoặc USB lạ không rõ nguồn gốc; Khi kết nối USB hãy giữ nhấn phím **SHIFT**; Nếu quên nhấn phím **SHIFT**, bạn hãy đóng bất cứ cửa sổ pop-up nào hiện ra khi USB được kết nối; Không mở bất cứ tệp tin nào trong ổ cứng hay USB mà bạn đang không tìm kiếm.

• Không tải các phần mềm độc hại

Nghĩ kỹ trước khi nháy chuột vào các liên kết đến các video clip, trò chơi, mở tệp ảnh và bài hát hoặc các tệp từ bất kỳ nguồn nào – kể cả từ người mà bạn tin tưởng. Hãy hỏi người gửi trước khi bạn mở tệp vì việc tải xuống có thể cài đặt những phần mềm độc hại hoặc kẻ xấu có thể đột nhập vào thiết bị của bạn.

• Cài đặt các ứng dụng bổ sung (add-in) một cách thận trọng

Một vài ứng dụng đó có thể gây hại cho máy tính hoặc ăn cắp các dữ liệu quan trọng. Hãy trung thành với các ứng dụng của những nhà cung cấp ứng dụng uy tín.

• Khóa điện thoại bằng mã số nhận dạng cá nhân (PIN)

Để người khác không thể dùng điện thoại của bạn để gọi, nhắn tin hoặc xem các thông tin cá nhân khác của bạn.

Câu hỏi luyện tập

Câu 1: Việc thiết lập trạng thái tự động cập nhật cho các phần mềm sẽ giúp bạn:

- ☐ a. Tiết kiệm được thời gian tìm và cập nhật các phiên bản mới cho các phần mềm.
- ☐ b. Luôn được cập nhật phần mềm mới nhất.
- ☐ c. Tránh được việc cập nhật nhầm các phần mềm chứa mã độc, virus gây hại cho máy tính.
- ☐ d. Cả 3 phương án trên.

Câu 2: Phát biểu sau đây Đúng (Đ) hay Sai (S) và tại sao?

a. Các đường link do người thân và bạn bè thân thiết gửi trực tuyến hoàn toàn an toàn vì đây là những người có thể tin tưởng tuyệt đối.

☐ **Đúng** ☐ **Sai**

b. Chỉ nên tải xuống (download) phần mềm ở những website của những đơn vị uy tín và có bản quyền khai thác sử dụng phần mềm đó.

☐ **Đúng** ☐ **Sai**

Câu 3: Nên đặt mã PIN cho máy tính hay điện thoại là:

- ☐ a. Ngày sinh nhật vì dễ nhớ
- ☐ b. Liên quan đến số điện thoại cá nhân
- ☐ c. Là tên riêng cho dễ nhớ
- ☐ d. Không nên đặt mã PIN liên quan đến các thông tin cá nhân vì dễ bị đoán và bị kẻ xấu lợi dụng mở điện thoại

2. Sử dụng thư điện tử an toàn (Email)

- **Sử dụng mật khẩu mạnh để bảo vệ email và các tài khoản trực tuyến khác.**

- Tạo mật khẩu dài (cụm hoặc câu) bao gồm cả chữ cái in hoa, chữ thường, số và ký tự.
- Tránh dùng cùng một mật khẩu cho tất cả các tài khoản. Vì nếu mật khẩu bị đánh cắp thì tất cả các tài khoản khác sẽ bị rò rỉ thông tin.
- Có thể lưu mật khẩu bằng cách viết ra giấy và lưu trữ cẩn thận, không chia sẻ mật khẩu với bất kỳ ai.

- **Dùng email một cách an toàn hơn.**

▶ Để ý các dấu hiệu gian lận:

+ Hãy thận trọng khi bạn nhận được những tin nhắn đầy bất ngờ như "bạn vừa trúng số độc đắc", hay cần phải gửi tiền cho người thân, hoặc giúp đỡ một người xa lạ chuyển tiền. Những dấu hiệu khác bao gồm việc thông báo đóng tài khoản, lỗi chính tả hoặc lỗi ngữ pháp.

+ Hãy tỉnh táo với những trò lừa đảo từ email, ví dụ một thư thông báo khẩn cấp có vẻ từ ngân hàng của bạn hoặc từ những tổ chức đáng tin cậy, như quỹ từ thiện mà bạn yêu thích. Chúng có thể yêu cầu bạn cung cấp mật khẩu, thông tin tài chính hoặc các thông tin nhạy cảm khác, hay yêu cầu bạn tới một trang web hoặc gọi tới một số điện thoại giả mạo.

Tìm hiểu thêm tại:
https://www.microsoft.com/en-us/safety/online-privacy/phishing-scams.aspx

▶ Suy nghĩ trước khi trả lời thư:

+ Hãy thận trọng kiểm tra tên của người gửi email cho bạn có thể là giả.
+ Hãy chú ý trước khi nháy chuột vào liên kết tới các videos, tệp hình ảnh, bài hát hoặc các tệp khác – kể cả khi bạn biết rõ về người gửi. Hãy hỏi người gửi trước khi bạn mở hoặc nhấp vào liên kết.

+ Hãy cảnh giác để không truy cập vào trang web hoặc gọi tới số điện thoại có trong tin nhắn khả nghi vì chúng có thể là giả mạo. Thay vào đó, chỉ liên hệ với địa chỉ mà bạn đã xác minh được chính xác.
+ Hãy cẩn thận với những gì bạn viết trong email vì chúng không được bảo mật và an toàn như viết trên một tấm bưu thiếp.

Câu hỏi luyện tập

Câu 1: Phát biểu sau đây Đúng (Đ) hay Sai (S) và tại sao?
Nên sử dụng chung mật khẩu (password) cho tất cả các tài khoản trực tuyến vì dễ quản lý và dễ ghi nhớ.

☐ **Đúng** ☐ **Sai**

Câu 2: Trong tình huống nhận được một email từ một người lạ, email có một tập tin đính kèm, bạn có nên mở email đó không? Hãy thảo luận với bạn bè để đưa ra phương án xử lý tình huống này.

Câu 3: Bạn nhận được email thông báo đã trúng thưởng may mắn từ chương trình X, chương trình yêu cầu bạn gửi lại địa chỉ nhà và số điện thoại để gửi giải thưởng cho bạn, bạn nên làm gì?

3. Sử dụng Mạng xã hội an toàn

- Xác định xem thông tin cá nhân hoặc blog của bạn nên đặt chế độ công khai như thế nào.

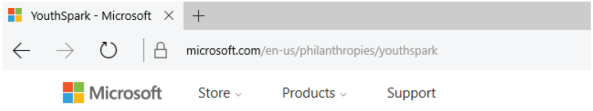
- Khi sử dụng các trang mạng xã hội hoặc viết blog, hãy cân nhắc về việc một số trang web sẽ tự động chuyển sang chế độ công khai cho tất cả người dùng Internet về những gì bạn đăng tải.

- Hãy tìm phần Cài đặt (Settings) hoặc Tùy chọn (Options) để quản lý ai có thể thấy thông tin cá nhân, hình ảnh, danh sách bạn bè, và mọi người có thể tìm ra trang cá nhân của bạn bằng cách nào, ai có thể bình luận hoặc làm sao để chặn những truy cập không mong muốn.

Một ví dụ cài đặt quyền riêng tư trên mạng xã hội Facebook

Bảo mật những thông tin cá nhân nhạy cảm.

- Trước khi nhập một thông tin nhạy cảm, hãy xem trang web đó có là địa chỉ web an toàn tin cậy hay không bằng cách tìm dấu hiệu https và biểu tượng khóa đóng ( ) bên cạnh.



Dấu hiệu https và biểu tượng khóa đóng khi mở website an toàn

- Không bao giờ cung cấp các thông tin nhạy cảm (như số tài khoản hay mật khẩu) hoặc gọi vào một số điện thoại theo yêu cầu trong email hoặc tin nhắn hay trên mạng xã hội.
- Suy nghĩ kỹ trước khi phản hồi cho việc xin tiền từ những đối tượng tự xưng là "thành viên gia đình", đó thường là một trò lừa đảo.

Nghiên cứu kỹ bất kỳ trang mạng xã hội nào trước khi bạn sử dụng chúng.

- Hãy đọc kỹ các điều khoản sử dụng. Trang web có quyền sở hữu thông tin của bạn không? Có thể bán thông tin của bạn không? Hoặc dùng những thông tin cá nhân của bạn để gửi thông tin quảng cáo không?
- Tìm hiểu khả năng quản lý những tương tác lạm dụng và nội dung không phù hợp của trang web, cũng cách thức báo cáo những vấn đề đó với trang web có được đảm bảo không.

Cẩn thận khi lựa chọn bạn bè trên mạng.

- Hãy nghĩ kỹ trước khi bạn chấp nhận lời mời kết bạn của ai đó. Chỉ nên kết bạn với những người mà bạn hoặc bạn thân của bạn đã gặp trực tiếp hoặc với những người mà bạn có bạn chung với họ.
- Định kỳ đánh giá lại những người có quyền truy cập vào thông tin của bạn. Danh sách bạn bè cũng có thể thay đổi theo thời gian.
- Kiểm tra lại những gì người khác viết về bạn. Hãy chắc chắn rằng họ không đăng những điều mà bạn không muốn chia sẻ như những bức ảnh cá nhân hoặc nơi ở của bạn. Bạn hoàn toàn có thể yêu cầu họ gỡ những thông tin đó xuống.

Hãy là một người bạn thực sự.

- Nếu như bạn không thực sự hiểu rõ một vấn đề nào đó, đừng chia sẻ nó lên mạng.
- Hãy đứng lên vì các bạn của mình. Bạo lực Internet ít dính đến những người có một nhóm bạn đoàn kết và sẽ bị ngăn chặn khi bạn bè của nạn nhân tập hợp lại.
- Không chia sẻ những thông tin cá nhân của bạn bè hoặc của gia đình lên mạng nếu chưa có sự cho phép của họ.

- Gặp một "người bạn" trên mạng có thể chất chứa đầy rủi ro. Hãy tự bảo vệ bản thân bằng cách luôn đi cùng một người lớn hoặc một người bạn mà bạn tin tưởng và gặp ở nơi công cộng đông người.

Nghĩ kỹ trước khi chia sẻ - không chia sẻ quá nhiều.

Trước khi bạn đăng tải bất kỳ thứ gì lên mạng, hãy nhớ rằng trang web có thể lưu trữ những điều bạn đăng, bạn bè có thể lấy nó về, hoặc kẻ xấu hoặc những lỗ hổng an ninh có thể lạm dụng nó.

- Đừng đăng bất kỳ những gì – đặc biệt là những thông tin nhạy cảm như địa chỉ nhà hay ngày sinh nhật – mà bạn chỉ có thể nói với bạn thân.
- Hãy cẩn thận khi chia sẻ cảm xúc – cho dù bạn đang vui, buồn, tức giận hoặc lo lắng về tiền bạc – vì nhiều người có thể khai thác những cảm xúc của bạn.
- Không đăng bất kỳ điều gì mà bạn thường chỉ có thể nói với bạn thân, bao gồm cả cảm xúc. Cho dù bạn vui, buồn, giận dữ hay có những mối lo lắng về tiền bạc, tâm sự rộng rãi có thể tăng nguy cơ bị xâm hại hoặc khiến bạn trở thành mục tiêu cho những trò lừa đảo.
- Hãy giữ những thông tin nhạy cảm cho riêng mình để không bị lừa đảo, mạo danh hoặc những người xấu có thể tìm thấy bạn qua địa chỉ nhà, số điện thoại hoặc tài khoản cá nhân, ngày sinh nhật và các bức ảnh.

- Cân nhắc đăng ảnh, video hoặc bình luận gợi ý. Hãy tự hỏi liệu chúng có thể ảnh hưởng xấu tới hình ảnh của bạn hay không.
- Nếu bạn sử dụng dịch vụ định vị, hãy xem xét việc giới hạn người biết vị trí của bạn. Chú ý tới địa điểm và thời gian bạn "check in", và cẩn trọng trong việc liên kết chúng tới các kênh mạng xã hội.
- Tạo mật khẩu mạnh và giữ chúng bí mật.

Các nguyên tắc tạo mật khẩu cho mạng xã hội hay bất cứ một tài khoản trực tuyến nào khác cũng giống như nguyên tắc tạo mật khẩu cho email mà bạn đã được tìm hiểu trong phần trước của cuốn cẩm nang này.

Câu hỏi luyện tập

Câu 1. Những phát biểu sau đây đúng (Đ) hay Sai (S)?

a. Có thể nói xấu về người khác trên mạng xã hội vì không ai biết bạn là ai ở ngoài đời thực.

☐ **Đúng** ☐ **Sai**

b. Nếu bạn biết một người bạn nào đó bị lan truyền thông tin xấu trên mạng xã hội, bạn không cần quan tâm vì đó không phải chuyện của bạn.

☐ **Đúng** ☐ **Sai**

c. Nếu bạn nói chuyện trực tuyến với một người có nhiều bạn bè chung với bạn, bạn có thể cho họ biết những thông tin cá nhân như địa chỉ, số điện thoại.

☐ **Đúng** ☐ **Sai**

Câu 2. Nếu bạn chia sẻ một hình ảnh lên mạng xã hội, nó sẽ tồn tại trên môi trường trực tuyến trong bao lâu?

- ☐ a. 3 tháng
- ☐ b. 6 tháng
- ☐ c. Đến khi bạn gỡ bỏ
- ☐ d. Có thể mãi mãi – người khác có thể lấy về và đăng tải lên bất cứ lúc nào

Câu 3. Hãy liệt kê 5 thông tin về bản thân mà bạn nghĩ rằng không nên chia sẻ trực tuyến?

.....

.....

.....

Câu 4: Bạn có thể gửi ảnh cho người khác trên môi trường trực tuyến trong trường hợp nào:

- ☐ a. Người đó gửi ảnh cho bạn trước
- ☐ b. Bạn gửi một bức ảnh đã cũ cho người đó
- ☐ c. Cho tới khi bạn cho họ biết địa chỉ
- ☐ d. Chỉ khi nào bố mẹ hoặc người lớn tin tưởng đồng ý cho bạn chuyển

Câu 5: Hãy thảo luận với bạn bè để đưa ra phương án cho những tình huống sau đây:

a. Nam và Cường kết bạn trên mạng xã hội và trò chuyện được vài tháng. Nam rủ Cường gặp mặt ngoài đời để hai bạn cùng đi chơi, Cường nên làm gì?
b. Thảo và Mai bắt đầu trò chuyện trên mạng xã hội vài ngày. Mai nói cho Thảo biết địa chỉ nhà, tuổi của Mai, trường học và Mai trông như thế nào. Mai hỏi Thảo địa chỉ trường học của Thảo ở đâu. Thảo nên làm như thế nào?
c. Toàn và Thắng là bạn trên mạng xã hội. Thắng giúp Toàn làm bài tập và hỏi số điện thoại của Toàn. Toàn có nên đồng ý không?

4. Sử dụng trình duyệt web an toàn

● Tìm những dấu hiệu cho thấy trang web đó an toàn.

- Đảm bảo bạn đang ở trang web đúng – ví dụ, khi đăng nhập vào trang web của ngân hàng, hãy đảm bảo đó không phải là trang giả mạo.
- Tìm các địa chỉ trang web có https (s viết tắt cho secure (an toàn)) và khóa đóng bên cạnh. (Khóa này cũng có thể xuất hiện phía dưới bên phải của cửa sổ). Không gõ thông tin nhạy cảm vào các cửa sổ web tự động xuất hiện.

● Tránh nhấp chuột vào các trạng thái "Agree", "OK" hoặc "I accept"

trên các banner quảng cáo, cửa sổ pop-up bất ngờ hiện ra với những cảnh báo hoặc đề nghị diệt vi rút và các phần mềm gián điệp, hoặc trên các trang web có vẻ bất hợp pháp và không chính thống.

- Thay vào đó, hãy nhấn **Ctrl + F4** hoặc **Ctrl + Alt** trên bàn phím để đóng các cửa sổ này lại.

- Nếu các cửa sổ này không đóng, hãy nhấn ALT + F4 trên bàn phím để đóng trình duyệt web lại. Đóng tất cả các tabs và không lưu lại bất cứ một tabs nào cho lần khởi động trình duyệt tiếp theo.

● Không tải các bản sao bất hợp pháp của âm nhạc, trò chơi video có bản quyền.

Các tập dữ liệu bất hợp pháp này thường được dùng để phát tán virus và phần mềm gián điệp với sự thiếu hiểu biết của người dùng.

- Đừng là một người gian lận trên mạng.

Không sao chép văn bản từ các trang web hoặc mua những bài luận văn, báo cáo hoàn chỉnh trên mạng.

Câu hỏi luyện tập

Câu 1: Trên môi trường trực tuyến, nếu bạn thấy một website làm bạn cảm thấy bất thường, không thoải mái (VD: tự động download phần mềm lạ, có dấu hiệu website giả mạo...), bạn nên làm gì?

- ☐ a. Ghi lại tên website này để không bao giờ quay trở lại.
- ☐ b. Nói với bạn bè để bạn bè cùng tránh.
- ☐ c. Tham khảo ý kiến bố mẹ, thầy cô hoặc người lớn đáng tin cậy.
- ☐ d. Tắt máy tính.

Câu 2: Các phát biểu sau đây là Đúng (Đ) hay Sai (S)

a. Khi mua sắm trực tuyến, luôn luôn cần kiểm tra lại xem trang web đó có cho phép chức năng thanh toán hợp pháp hay không.

☐ **Đúng** ☐ **Sai**

b. Khi làm khảo sát trực tuyến, không cần xin phép người lớn, mà chỉ cần trả lời vui đùa không trung thực để không lộ thông tin cá nhân.

☐ **Đúng** ☐ **Sai**

5. Hành động khi xảy ra vấn đề

Trong trường hợp bạn bị xâm hại trên môi trường trực tuyến, hãy lưu lại các bằng chứng bất cứ khi nào có thể.

- **Khi sử dụng email, mạng xã hội hay dịch vụ web.**

- Nếu bạn gặp phải bất kỳ sự lừa đảo, các nội dung xúc phạm hoặc lợi dụng vị thành viên, hành vi đe dọa hoặc trộm cắp tài khoản, hãy báo cáo điều này. Ví dụ, tìm đường dẫn báo cáo lạm dụng (Report Abuse) trong phần dịch vụ hoặc phần mềm của Microsoft, hoặc liên hệ với ban quản trị tại *https://cert.microsoft.com/report.aspx*
- Nếu ai đó lấy tài khoản email của bạn, hãy thay đổi mật khẩu ngay tức khắc (nếu có thể) hoặc báo cáo sự việc với nhà cung cấp email của bạn.

- **Bị quấy rối liên tục hoặc bị xâm phạm về thân thể.**

Báo cáo với các cơ quan chức năng có thẩm quyền tại địa phương và các đơn vị bảo vệ quyền lợi cho trẻ em.

- **Danh tính của bạn bị đánh cắp hoặc bạn đã lỡ dính vào một vụ lừa đảo qua mạng (scam).**

Hãy thay đổi ngay lập tức mật khẩu và số nhận dạng cá nhân ở tất cả các tài khoản, và báo cáo:

- Với công ty thẻ tín dụng, ngân hàng, hoặc công ty bảo hiểm sức khỏe của bạn.
- Với các cơ quan chức năng có thẩm quyền tại địa phương.
- Với các tổ chức bảo vệ quyền lợi cho trẻ em tại địa phương.

PHẦN II:

DÀNH CHO PHỤ HUYNH

I. Tại sao phụ huynh cần hướng dẫn và bảo vệ trẻ về an toàn sử dụng Internet

Kể từ khi con trẻ chập chững biết đi, bạn đã cần hướng dẫn cho trẻ làm thế nào để đảm bảo sự an toàn trong đời sống hàng ngày. Vậy còn an toàn sử dụng Internet thì sao? Bố mẹ hãy bắt đầu bằng việc tìm hiểu những mối nguy hiểm có thể xảy đến với trẻ nhỏ trên môi trường trực tuyến.

Trẻ có thể vô tình để lộ thông tin cá nhân trên môi trường trực tuyến nhiều hơn mức cần thiết. Rất nhiều trẻ nhỏ đưa ra những thông tin có thể ảnh hưởng đến hình ảnh cá nhân và có những hậu quả tiêu cực trong suốt thời gian dài về sau. Các em cũng có thể dễ dàng chia sẻ mật khẩu hoặc những thông tin cá nhân trên mạng xã hội hoặc thông tin tiết lộ về bản thân hay địa chỉ cá nhân. Điều này có thể dẫn tới những xâm phạm, lừa đảo, trộm cắp hoặc những lợi dụng của kẻ xấu đối với trẻ nhỏ.

Trẻ nhỏ tham gia môi trường trực tuyến mà không nhận thức được bài hát, trò chơi hoặc video từ những trang web hoặc những nguồn chia sẻ thông tin miễn phí không quen thuộc có thể có nhiều ảnh hưởng tiêu cực. Máy tính có thể bị tấn công bởi những phần mềm độc hại, những thông tin cá nhân bị xâm hại. Sử dụng webcam và camera của điện thoại cũng có thể dẫn tới những hành vi chứa đựng nhiều rủi ro.

Những kẻ xấu lợi dụng để tiết lộ thông tin cá nhân của trẻ nhỏ. Những website ở câu lạc bộ hoặc trường học có thể lưu trữ rất nhiều thông tin của học sinh và thành viên. Gia đình và bạn bè có thể cũng tương tác với trẻ nhỏ thông qua những bức hình hay bình luận. Một vài trang thông tin sẽ bán những thông tin cá nhân mà họ thu thập được.

Các dịch vụ trực tuyến cũng có thể khiến trẻ nhỏ vào những mối nguy hiểm vì khi sử dụng các dịch vụ này trẻ nhỏ sẽ để lộ nhiều thông tin cá nhân một cách không cẩn trọng, trong khi các dịch vụ đó không đảm bảo được sự an toàn bảo mật cho người dùng.

II. Làm thế nào để bảo vệ trẻ an toàn trên môi trường trực tuyến

1. Đặt vấn đề với trẻ về an toàn sử dụng Internet

- Với những trẻ dưới 10 tuổi: Cách tiếp cận tốt nhất là bạn ngồi xuống và cùng tham gia vào các hoạt động trên mạng của các con, cởi mở với những câu hỏi và sự tò mò của trẻ. Khi chúng lớn hơn, giúp chúng sử dụng những dịch vụ và các công cụ mới trên Internet.

- Với trẻ từ 10 - 15 tuổi: Cách hiệu quả nhất là hướng dẫn, trao đổi cởi mở và tích cực. Gợi ý để chúng chia sẻ với bạn những trang mà chúng truy cập, hay chúng tạo ra, những trò chơi mà chúng chơi, những gì và những ai chúng trò chuyện.

Từ đó, hãy thống nhất với trẻ và đưa ra những nguyên tắc khi trẻ sử dụng Internet:

+ Thảo luận về các loại trang web, apps, tính năng điện thoại hay trò chơi mà chúng có thể sử dụng, phù hợp với lứa tuổi, sự trưởng thành và các giá trị của gia đình. Thảo luận liệu con bạn có nên được phép mua bán online hay không.

+ Nói chuyện về những thông tin phải giữ bí mật, thời lượng sử dụng Internet, và hướng dẫn để trẻ giao tiếp văn minh.

+ Nếu bạn có ý định giám sát con mình bằng những thiết bị an ninh trong gia đình như camera, giải thích cho con hiểu vì sao và con sẽ phải làm gì.

+ Xem lại những quy tắc trên thường xuyên, dựa vào sự trưởng thành của con bạn và sự phát triển của thiết bị và công nghệ.

2. Trao đổi với trẻ những nội dung thiết thực để đảm bảo an toàn sử dụng Internet

2.1. Suy nghĩ trước khi nhấp chuột

- Khi đứa trẻ nhận được những tin nhắn không được tôn trọng hay không bình thường, ngay cả khi chúng đến từ những người bạn, hãy nói với chúng không được mở ảnh, bài hát hay tệp đính kèm hay nhấp vào những đường link trong tin nhắn đó. Thay vào đó, chúng nên kiểm tra với người gửi bằng một phương tiện nào đó hơn là việc nhấp vào mục "Trả lời".

- Nói chuyện với con bạn về việc chỉ tải xuống những phần mềm, trò chơi, nhạc và những nội dung hợp pháp.

2.2. Hãy tỉnh táo với điện thoại di động

- Giúp con bạn khóa máy điện thoại bằng mật khẩu mà chúng có thể giữ bí mật ngay cả với những người bạn thân nhất.
- Giúp đỡ trẻ quản lý các địa chỉ liên lạc của chúng, có thể hạn chế tiếp xúc chỉ với những số được cho phép. Con bạn chỉ nên chia sẻ những số liên lạc của chúng với những người mà chúng biết rõ trực tiếp, mà không phải chỉ trên trang thông tin cá nhân của họ.
- Dạy con bạn sử dụng GPS thận trọng vì nó có thể được sử dụng để xác định nơi chúng đang ở hay vị trí nơi bọn trẻ chụp ảnh.

2.3. Hãy chơi một cách an toàn

Tìm hiểu những trò chơi mà trẻ muốn chơi. Kiểm tra đánh giá và chọn những trò chơi nổi tiếng và từ các trang web uy tín. Hãy cùng lập những hướng dẫn trong gia đình cho việc chơi trò chơi:
- Liệu trẻ em nên chơi trò chơi chỉ có một mình? Hay chỉ với bạn? Hay với ai đó?
- Bao nhiêu tiếng một ngày hay một tuần là phù hợp?
- Chúng có sẵn sàng sử dụng những tính năng tin nhắn văn bản, thoại hay webcam? Nếu có thì với ai?

2.4. Hãy suy nghĩ trước khi sử dụng ứng dụng

- Giúp con bạn lựa chọn ứng dụng phù hợp với lứa tuổi và mức độ trưởng thành của chúng.
- Dùng những ứng dụng được đánh giá là tốt, và từ những đơn vị cung cấp có uy tín.
- Cùng nhau xem lại những chính sách bảo mật để xem ứng dụng sẽ làm gì với việc định vị và những dữ liệu nhạy cảm khác không.

2.5. Chia sẻ với sự cẩn trọng

- Dạy con bạn không chia sẻ dữ liệu cá nhân trên mạng như tuổi, số điện thoại, tên đầy đủ, hình ảnh, địa chỉ nhà riêng và email, thậm chí cả cảm xúc – với bất kỳ ai trừ những người bạn thân.
- Hãy làm rõ với bọn trẻ rằng chúng không bao giờ nên nói, nhắn tin hay đăng tải bất kỳ điều gì sẽ làm tổn thương hay làm ai xấu hổ. Không bắt nạt người khác.
- Nhấn mạnh rằng chúng không nên làm, gửi hay chấp nhận những tin nhắn, hình ảnh hay video mang tính khiêu dâm.

2.6. Hỗ trợ con kết nối với mạng xã hội an toàn

- Hãy chỉ cho con bạn làm thế nào để làm cho các trang mạng xã hội có tính riêng tư.
- Yêu cầu con bạn hãy suy nghĩ ít nhất 2 lần trước khi nó kết bạn với một ai. Hãy cân nhắc chỉ kết bạn với những người mà chúng hoặc những người bạn thân của chúng đã gặp mặt trực tiếp hoặc với những người chúng có những người bạn chung.
- Khuyến khích con bạn sử dụng những hình ảnh tích cực trên mạng, và tôn trọng các bình luận.

3. Sử dụng một vài cách khác để trẻ lên mạng an toàn hơn

Hãy coi an toàn trên mạng là một nỗ lực của cả gia đình, là sự kết hợp giữa hướng dẫn và giám sát liên tục.

- Đàm phán với trẻ và hướng dẫn rõ ràng cho việc sử dụng website và trò chơi trực tuyến phù hợp với lứa tuổi của trẻ và những giá trị của gia đình bạn.
- Chú ý tới những gì trẻ làm và những người chúng gặp trên mạng.
- Quan sát những dấu hiệu bị bạo lực trên mạng như trẻ thấy khó chịu khi lên mạng hay miễn cưỡng khi đi học.
- Hãy là người quản trị máy tính của gia đình. Sử dụng các thiết bị an ninh trong gia đình để giúp bạn theo dõi những gì bọn trẻ đang làm trên mạng.

4. Hành động khi xảy ra vấn đề

- **Dạy trẻ tin tưởng vào bố mẹ và người thân**

Hãy để chúng biết rằng chúng có thể tìm đến bạn để giúp giải quyết vấn đề. Làm rõ rằng bạn sẽ không phạt chúng hay cắt quyền sử dụng máy vi tính, trò chơi hay điện thoại chỉ vì sai lầm của người khác.

- **Báo cáo ngay lập tức nếu đứa trẻ đang gặp nguy hiểm ngay trước mắt như ai đó đe dọa, quấy rối, hay cố gắng thuyết phục trẻ gặp mặt trực tiếp**

- Báo cáo mối đe dọa thể chất, bạo lực internet hay bất kỳ sự lạm dụng nào với đơn vị có thẩm quyền tại địa phương.
- Báo cáo những hành động cư xử không đúng đắn, như bạo lực internet với nhà trường (nếu việc này liên quan đến học sinh khác), và tới hãng điện thoại hay nhà cung cấp web. Ví dụ, trong các dịch vụ và phần mềm của Microsoft, hãy tìm tới đường dẫn Report Abuse (Báo cáo lạm dụng), hoặc liên lạc với nhà cung cấp dịch vụ tại:

https://cert.microsoft.com/report.aspx

ĐÁP ÁN CÂU HỎI LUYỆN TẬP

1. Bảo vệ máy tính và các thiết bị điện tử an toàn (Trang 7).

Câu 1: d

Câu 2:

a. Sai. Ngay cả khi người thân hay bạn bè thân thiết gửi cho bạn những đường dẫn trực tuyến, bạn cũng không nên vội vàng nhấp chuột vào, vì tài khoản của những người này có khả năng đã nhiễm virus từ trước đó. Vì vậy bạn hãy xác nhận lại với họ về việc họ có ý định gửi nội dung nào đó cho bạn hay không.

b.Đúng.

Câu 3: d

2. Sử dụng Email an toàn (Trang 9)

Câu 1: Sai. Không nên đặt chung mật khẩu cho tất cả các loại tài khoản. Trong trường hợp mật khẩu của bạn bị lấy mất, kẻ trộm có thể dùng mật khẩu này để đăng nhập vào tất cả các tài khoản trực tuyến của bạn, khiến hậu quả trở nên trầm trọng hơn.

Câu 2: Không nên mở email từ một người lạ có tập tin đính kèm, rất có thể tập đính kèm đó chính là tập tin độc hại có chứa virus. Hãy kiểm tra lại thông tin của người gửi email trước để xem bạn có thể có mối liên hệ nào đó với người gửi hay không, có thể tin tưởng được người gửi thư cho bạn hay không.

Câu 3: Không nên vội vàng trả lời email của cá nhân hay đơn vị không quen biết, đặc biệt là những email yêu cầu bạn cung cấp thông tin cá nhân. Trong trường hợp này, bạn có thể nói chuyện với người lớn hoặc tra cứu các thông tin về chương trình X để xác thực thông tin có chính xác hay không trước khi gửi email trả lời.

3. Sử dụng Mạng xã hội an toàn (Trang 13, 14)

Câu 1:

a. Sai

b. Sai

c. Sai

Câu 2: d

Câu 3: 5 thông tin có thể thuộc các nội dung: họ và tên, địa chỉ, số điện thoại, tên trường học, tuổi, ngày sinh, địa điểm, địa chỉ email, mật khẩu, cuộc hội thoại cá nhân.

Câu 4: d

Câu 5:

a. Cường nên nói chuyện này với người lớn như bố mẹ, anh chị...Khi tới gặp mặt Nam, Cường nên có người lớn đi cùng để đảm bảo rằng Nam là người bạn tốt và đáng tin tưởng để gặp gỡ ngoài đời.

b. Thảo nên kể cho người lớn và hỏi ý kiến bố mẹ, người thân trước khi cho thông tin cá nhân của mình cho Mai.

c. Toàn không nên cho số điện thoại Thắng để Thắng làm bài tập giúp. Toàn nên tự làm bài tập và nhờ sự gợi ý của bố mẹ, thầy cô, bạn bè nếu cần. Toàn cũng nên nói với bố mẹ về việc Thắng hỏi xin số điện thoại. Không nên cho số điện thoại hay bất cứ thông tin cá nhân nào bạn gặp trên mạng xã hội mà không rõ họ là ai và có đáng tin tưởng hay không.

4. Sử dụng Website an toàn (Trang 16)

Câu 1: c. Hãy nói với người thân, bạn bè và những người lớn tin tưởng để đưa ra những giải pháp hợp lý nhất, xem xét xem trang web đó có thực sự là trang web xấu không, trong trường hợp có thể báo cáo với các cơ quan có thẩm quyền để quản lý và xử lý nếu có vi phạm xảy ra.

Câu 2:

a. Đúng

b. Sai. Khi làm khảo sát trực tuyến, hãy trả lời trung thực các câu hỏi, nhưng trước khi tham gia khảo sát, hãy xin phép ý kiến bố mẹ, thầy cô và những người lớn đáng tin cậy.

PHỤ LỤC 1

PHOTODNA

PHOTODNA – CÔNG CỤ HỮU HIỆU CHỐNG XÂM HẠI TRẺ EM

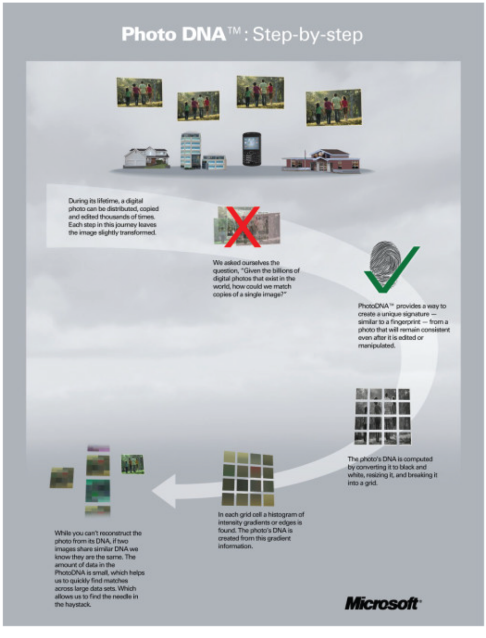
Hãy tưởng tượng chúng ta là những bác sĩ, nhiệm vụ của chúng ta là cần tìm ra căn bệnh mà bệnh nhân mắc phải trong khi không có những thiết bị y tế và công nghệ xét nghiệm hiện đại như ngày nay. Tình huống trở nên thật khó khăn vì bằng một cách nào đó, chúng ta vẫn phải nhận biết căn bệnh và đưa ra những phương thuốc ngăn chặn trước khi tình trạng trở nên tồi tệ hơn.

Tương tự như vậy, đối với những đơn vị cung cấp dịch vụ chia sẻ hình ảnh hay mạng xã hội, việc ngăn chặn những bức ảnh bất hợp pháp của những thiếu niên và các em bé nhằm mục đích tống tiền và lạm dụng tình dục chỉ trở nên bớt phức tạp và không còn khó khăn khi họ có trong tay những công cụ hữu hiệu. Hiện nay trên thế giới mỗi ngày có khoảng 720,000 bức ảnh bất hợp pháp trong khoảng 1,8 tỷ bức ảnh được chia sẻ trên môi trường trực tuyến, và tình trạng này càng trở nên khó kiểm soát hơn bao giờ hết.

Trong bối cảnh đó, việc đưa ra PhotoDNA – dịch vụ miễn phí giúp nhận biết và loại trừ những bức ảnh bất hợp pháp chính là một trong những cam kết của Microsoft về việc mang lại những giải pháp giúp cộng đồng được an toàn hơn khi trải nghiệm trực tuyến, đặc biệt là có thể an tâm trước những sự cố ngoài mong muốn, tải về các nội dung bất hợp pháp và phải nhận những nội dung không mong đợi.

PhotoDNA là một trong những yếu tố cơ bản nhất trong chiến lược bảo vệ khách hàng, bảo vệ các hệ thống và danh tiếng của Microsoft, thông qua việc hỗ trợ tạo ra một môi trường trực tuyến an toàn hơn. Kể từ năm 2009, Microsoft và Đại học Dartmouth đã cùng hợp tác phát triển công nghệ này nhằm mục tiêu tìm kiếm và loại trừ những bức ảnh "tệ nhất trong những bức hình tồi tệ" của những trẻ em bị lạm dụng tình dục trên Internet. Microsoft đã hiến tặng công nghệ PhotoDNA cho Trung tâm Quốc gia về Trẻ em bị mất

tích và bóc lột (National Center for Missing & Exploited Children - NCMEC), tổ chức này đã thành lập chương trình hỗ trợ các nhà cung cấp dịch vụ trực tuyến, nhằm giúp họ ngăn chặn việc phát tán các tư liệu của các em bé bị lạm dụng tình dục trên mạng.



Đồ hình về tiếp cận của công nghệ Microsoft PhotoDNA

Hiện nay, PhotoDNA đã trở thành một trong những công cụ thực tế tốt nhất chống lại tệ nạn lạm dụng tình dục trẻ em trên Internet. PhotoDNA đang được cung cấp miễn phí cho các công ty và các nhà phát triển ứng dụng đủ tiêu chuẩn. Hiện nay, hơn 70 công ty lớn, bao gồm cả Google, Facebook và Twistter, các tổ chức phi chính phủ và các đơn vị thực thi pháp luật đang sử dụng công nghệ PhotoDNA.

Công nghệ PhotoDNA chuyển đổi hình ảnh sang định dạng điểm ảnh đen trắng (greyscale) và có kích cỡ đồng nhất, từ đó sẽ phân nhỏ hình ảnh thành các ô vuông, gán giá trị số độc nhất cho từng phần màu sắc tìm được trong những ô vuông đó. Khi kết hợp với nhau, những con số này đại diện cho một "chữ ký PhotoDNA" hoặc chữ ký hình ảnh, nhờ đó chúng ta có thể so sánh các chữ ký với những hình ảnh khác để tìm kiếm những bản sao của hình ảnh được cung cấp với độ chính xác đáng kinh ngạc. Thông tin chi tiết về công nghệ Photo DNA có tại: *www.microsoft.com/photodna.*

PHỤ LỤC 2

CÁC PHẦN MỀM MIỄN PHÍ BẢO VỆ WINDOWS TỐT NHẤT

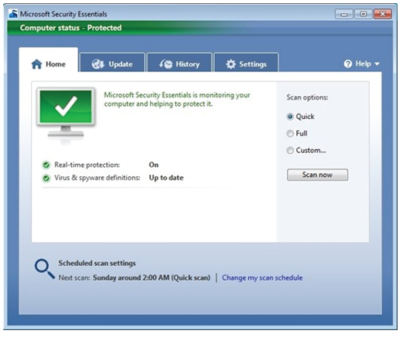
Nếu đang sử dụng hệ điều hành Windows thì bạn có thể hiểu được rằng nền tảng này sở hữu số lượng ứng dụng cũng như tính năng cực kỳ đa dạng và phong phú. Chính vì vậy, nhà cung cấp Microsoft cũng phát hành rất nhiều bộ công cụ miễn phí để người dùng kiểm soát cũng như khắc phục tốt các lỗi nảy sinh trong quá trình sử dụng.

Ưu điểm của việc sử dụng các công cụ miễn phí từ Microsoft là tính tương thích tốt hơn với Windows khi so sánh với các công cụ của bên thứ ba. Do đó, không có lý do gì người dùng có thể bỏ qua những tiện ích này để giúp chiếc máy tính của mình có thể chống lại các phần mềm độc hại, quản lý tài nguyên hệ thống hay khắc phục những trục trặc nhanh nhất có thể.

Dưới đây là 8 công cụ được Microsoft cung cấp miễn phí mà người dùng Windows không nên bỏ qua:

• Security Essentials

Microsoft Security Essentials (MSE) là công cụ bảo mật miễn phí, gọn nhẹ, có nhiệm vụ bảo vệ người dùng khỏi các loại virus và spyware, bao gồm cả trojan, worm và các loại phần mềm độc hại khác.



Phần mềm có khả năng tương thích rất tốt với hệ điều hành Windows cũng như có khả năng nhận dạng tốt các phần mềm gây hại. Nếu bạn đang sử dụng Windows 8 thì MSE đã được tích hợp sẵn. Đặc biệt, MSE có thể tải xuống miễn phí từ Microsoft, cài đặt đơn giản, dễ sử dụng và luôn được cập nhật để bạn có thể yên tâm rằng máy tính của mình được bảo vệ bằng công nghệ mới nhất.

MSE hoạt động ẩn trên nền một cách có hiệu quả, do vậy, bạn có thể thoải mái sử dụng máy tính chạy hệ điều hành Windows của mình như mong muốn mà không bị gián đoạn hay mất thời gian chờ lâu.

Ngoài ra, MSE có chế độ bảo vệ máy tính theo thời gian thực, giúp ngăn chặn các phần mềm độc hại trước khi chúng có cơ hội gây ra rắc rối. Tính năng Dynamic Signature Service, tương tự như tường lửa, quản lý các kết nối, chống lại các kết nối trái phép từ bên ngoài, kiểm tra các phần mềm tự kích hoạt…

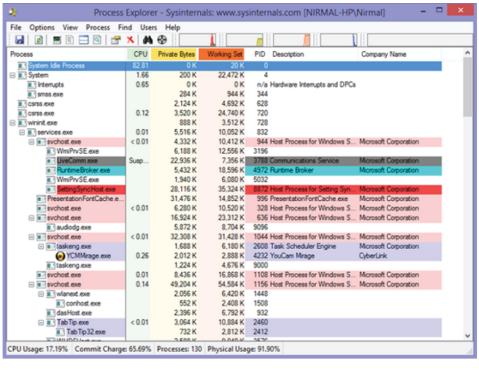
Sysinternals Suite

Đây thực chất là bộ công cụ đã được cải tiến và tổng hợp lại của Sysinternals Troubleshooting Utilities, tác giả không ai khác chính là Mark Russinovich, chuyên gia hệ thống công nghệ và bảo mật hàng đầu của Microsoft.

Tất cả những những phần mềm hệ thống nổi tiếng như Autoruns, Process Explorer, FileMon, RegMon, TCPView,… sẽ đều góp mặt trong Sysinternals Suite. Hiện tại, Sysinternals Suite hỗ trợ tới trên 65 công cụ, giúp cho bạn có thể thao tác, theo dõi và quản lí hệ thống một cách toàn diện.

Process Explorer

Nếu máy tính của bạn hay bị treo vì sử dụng quá nhiều tài nguyên, bạn cần giảm tải cho bộ vi xử lý bằng cách tắt bớt các quy trình không cần thiết. Tiện ích Process Explorer được tạo ra để giúp bạn thực hiện điều đó.

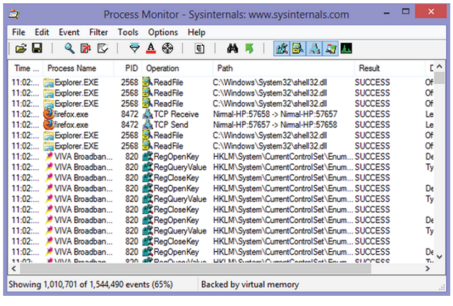


Process Explorer cung cấp thông tin một cách khá chi tiết về từng tiến trình và dịch vụ cũng như chỉ ra những ứng dụng nào liên quan đến nó. Nhờ vậy, bạn có thể tắt các dịch vụ một cách an toàn mà không ảnh hưởng đến ứng dụng đang chạy. Công cụ này cũng giúp bạn phát hiện ra những chứng cứ để cho thấy một tiến trình hay dịch vụ là phần mềm gián điệp hay phần mềm độc hại.

Process Monitor

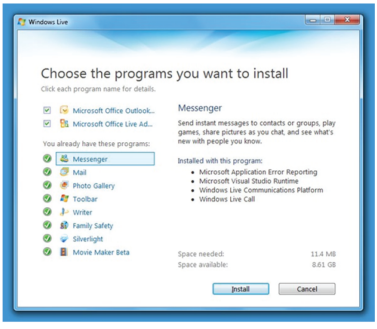
Process Monitor là tiện ích theo dõi chi tiết những hành động đang xảy ra với hệ thống file, registry, những tiến trình (process) và luồng dữ liệu (thread) trên hệ điều hành Windows. Nó tổng hợp 2 tiện ích rất nổi tiếng của hãng Sysinternals là Filemon và Regmon, đồng thời tích hợp thêm 1 danh sách các chức năng mở rộng bao gồm việc lọc, hiển thị thông tin chi tiết như session ID và tên người dùng, hiển thị đầy đủ luồng dữ liệu với những kí hiệu mô tả từng hoạt động và ghi lịch sử các hoạt động trên hệ thống vào file, …

Những tính năng mạnh mẽ và độc nhất này đã làm Process Monitor trở thành một tiện ích không thể thiếu trước các vấn đề của hệ thống và tiêu diệt các phần mềm độc hại.



Windows Essentials

Windows Essentials là một gói các chương trình miễn phí dành cho chiếc PC chạy Windows của bạn bao gồm Windows Live Mail, Family Safety, Live Writer, Messenger (nay là Skype) hay thư viện ảnh...



OneDrive

Về cơ bản, dịch vụ lưu trữ dữ liệu trực tuyến miễn phí của Microsoft này hoạt động tương tự như Dropbox, Google Drive ... Người dùng Windows sau khi cài đặt ứng dụng OneDrive vào máy tính của mình chỉ cần đăng nhập vào tài khoản Windows Live để liên kết máy tính đang sử dụng với dịch vụ lưu trữ trực tuyến này.

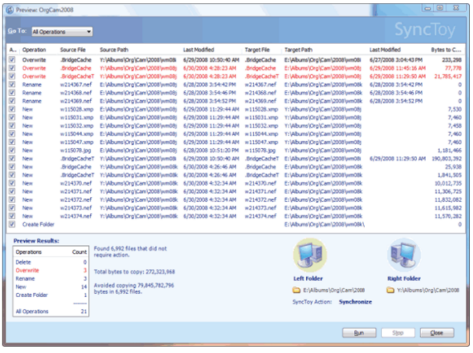
OneDrive sẽ tạo ra một thư mục riêng trong máy tính của người dùng. Việc đồng bộ hóa tất cả các tập tin và thư mục được lưu trong OneDrive sẽ được thực hiện ngay lập tức và hoàn toàn tự động, mọi tập tin có trong OneDrive của người dùng sẽ được lưu trong thư mục OneDive trên máy tính cũng như được lưu trên mây.

OneDrive cung cấp cho người dùng 5 GB không gian lưu trữ miễn phí cùng với các tùy chọn nâng cấp lên 50 GB, 1 TB, 5 TB với một phí trọn gói hàng tháng. Mặc dù có logo Microsoft nhưng OneDrive là một nền tảng cho phép bạn có thể truy cập tập tin lưu trữ thông qua cả các ứng dụng trên điện thoại Android, iOS và bất kỳ thiết bị nào, chỉ với một trình duyệt web, nhưng tốt nhất dĩ nhiên vẫn là với hệ điều hành Windows.

SyncToy

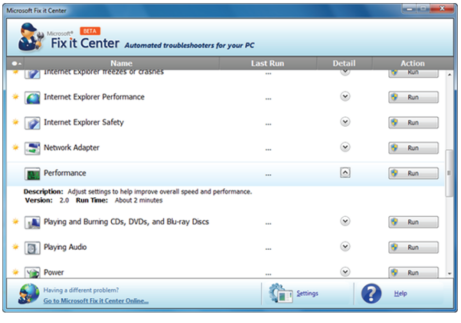
SynToy là một phần mềm miễn phí do Microsoft phát triển, có chức năng đồng bộ hóa, sao chép và sao lưu dữ liệu. Nguyên tắc cơ bản là để dữ liệu giữa các vị trí (thư mục, ổ đĩa cứng và ổ USB…) luôn được cập nhật mới nhất, tránh thiếu sót dữ liệu, đồng thời tạo lập phương án dự phòng khôi phục dữ liệu trong trường hợp dữ liệu ở một vị trí gặp sự cố (xóa nhầm, bị virus phá hoại...). Cụ thể, người dùng có thể đồng bộ dữ liệu của hai thư mục nằm ở hai ổ đĩa, giữa máy tính và ổ đĩa USB, giữa hai máy tính…

SyncToy sử dụng một phương pháp mới cho việc đồng bộ, phương pháp này mang tên Folder Pairs. Thay vì định nghĩa một cách đại thể về các tùy chọn đồng bộ của bạn là gì và sau đó là việc lựa chọn các thư mục riêng rẽ, bạn có thể quyết định những thư mục nào muốn đồng bộ và sẽ được đồng bộ theo cách nào.



Microsoft Fix it

Có trong tay công cụ Microsoft Fix it, hầu hết trục trặc liên quan đến hệ điều hành Windows sẽ được giải quyết gọn lẹ. Chuyên trang Microsoft Fix it Solution Center được Microsoft cho ra đời nhằm giải đáp thắc mắc và cung cấp giải pháp giúp người dùng giải quyết các vấn đề liên quan đến Windows, kèm theo tiện ích Microsoft Fix it giúp tự động khắc phục vấn đề tương ứng. Tuy nhiên, nếu không rành rẽ về công nghệ thông tin, bạn phải tốn không ít thời gian nếu muốn tìm thấy "liều thuốc" trị "căn bệnh" mà Windows mắc phải.



Thấu hiểu điều này nên Microsoft đã phát hành công cụ Microsoft Fix It, có khả năng tự động tìm và chuẩn đoán hầu hết lỗi "kinh điển" cho Windows XP SP3/XP Pro SP2 64-bit/Vista/ 2003 SP2/-Server 2008/ Server 2008 R2 hoặc Windows 7 dựa trên cơ sở dữ liệu của trang web Microsoft Fix it Solution Center.

MỤC LỤC

Tài liệu được biên soạn bởi Trung tâm Công nghệ thông tin – Truyền thông Vietnet
Tài liệu gốc cung cấp bởi Microsoft tại:
https://www.microsoft.com/about/philanthropies/youthspark/youthsparkhub

CẨM NANG AN TOÀN SỬ DỤNG INTERNET

- Bảo vệ các thiết bị kết nối Internet (máy tính, điện thoại).
- Sử dụng thư điện tử an toàn (Email).
- Sử dụng Mạng xã hội an toàn.
- Sử dụng trình duyệt web an toàn.
- Hành động khi xảy ra vấn đề.