**1.Chữ ký điện tử là gì?**

Chữ ký số là một dạng chữ ký điện tử. Chữ ký số được tạo ra bởi người ký đóng vai trò như chữ ký đối với cá nhân hay con dấu đối với doanh nghiệp và được thừa nhận về mặt pháp lý. Chữ ký số được coi là phương án giải quyết tốt nhất mọi vấn đề khi giao dịch trên môi trường Internet và còn được ứng dụng vào nhiều lĩnh vực bảo mật cao khác.

**2.Các chương trình diệt virus ?**

**2.1 Phần mềm diệt virus là gì?**

Phần mềm diệt virus là phần mềm có tính năng phát hiện, loại bỏ các virus máy tính, khắc phục (một phần hoặc hoàn toàn) hậu quả của virus gây ra và có khả năng được nâng cấp để nhận biết các loại virus trong tương lai.

**2.2 Các phầm mềm diệt virus phổ biến**

Phần mềm diệt virus Avira Free Antivirus 2018

Phần mềm diệt virus Avira Free Antivirus 2018 là một sản phẩm của công ty bảo mật Avira Operations GmbH. Những sản phẩm diệt virus miễn phí của hãng này đều rất tốt. Riêng mình trước khi sử dụng trả phí mình toàn sử dụng miễn phí của thằng này. (Hiện tại mình dùng trả phí của Kaspersky)

– Ưu điểm của ***phần mềm diệt virus*** này là khi sử dụng phần mềm chiếm rất ít tài nguyên và điểm nổi trội của Avira Free 2018 chính là tặng bạn 5GB dung lượng để sao lưu dữ liệu trực tuyến. Ngoài ra nó cung cấp thanh công cụ Avira Search Free Toolbar được cài đặt lên trình duyệt web của bạn, giúp bạn duyệt web an toàn hơn.

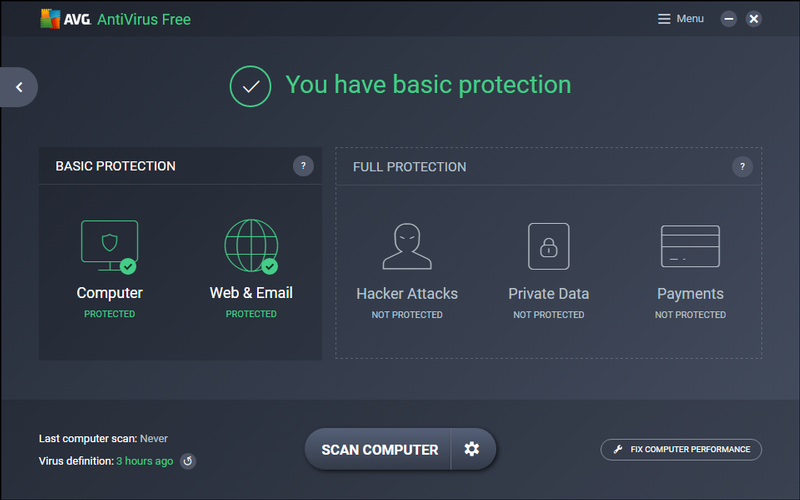
**Những ưu điểm của phần mềm diệt virus miễn phí Avira Antivirus 2018**

* Giao diện đơn giản, trực quan, tối ưu với người dùng
* Bảo vệ các dữ liệu cá nhân, các thông tin và mật khẩu
* Quét virus với công nghệ điện toán đám mây.
* Cảnh báo và chặn những trang web chứa virus khi bạn truy cập vào những website đó

## 2: Phần mềm diệt Virus miễn phí của AVG

AVG là thương hiệu diệt virus có từ rất lâu đời. Ngoài những phiên bản trả phí của AVG thì AVG cũng có phiên bản miễn phí với công nghệ điện toán đám mây hiện đại tạo môi trường an toàn và nâng cao hiệu suất sử dụng máy tính của bạn.

Hiện tại AVG cung cấp 2 giải pháp quét đó là quét toàn bộ ổ cứng và quét theo từng thư mục. AVG sẽ phát hiện những file bị nghi là virus và đem vào phân tích và đảm bảo được máy tính của bạn tốt nhất

[](http://congnghe3s.com/wp-content/uploads/2013/10/avg-antivirus-2018-free.png)

Giao diện của Avg Antivirus Free 2018

### 3 lý do dể bạn sử dụng AVG AntiVirus miễn phí

Hiện nay trên thế giới hang triệu người đã tin tưởng và sử dụng **phần mềm diệt virus** này để bảo vệ máy tính của mình bởi vì đây là một phiên bản miễn phí nhưng chất lượng của nó không hề kém ( Theo mìnhd đánh giá còn hơn) những phiên bản trả phí của nhà cung cấp khác. AVG Free AntiVirus được cài đặt rất nhanh và nó sẽ bảo vệ máy tính của bạn mãi mãi với công nghệ bảo vệ 2 lớp. Ngoài ra nó cũng rất nhẹ và không làm ảnh hưởng đến tốc độ máy tính của bạn

Bảo vệ máy tính theo thời gian thực giúp bạn không bị virus, spyware, ransomware, rootkit, Trojan và các phần mềm độc hại khó chịu. Với công nghệ trí tuệ nhân tạo theo dõi theo thời gian thực giúp bạn bảo vệ máy tính toàn diện.

Bảo vệ website và Email: AVG Antivirus Free còn cung cấp khả năng bảo vệ trực tuyết khi bạn click vào những liên kết độc hại, ví dụ những virus được gửi qua facebook hay email sẽ khiến máy tính bạn nhiễm virus khiến bạn bị người khác chiếm mất quyền sử dụng tài khoản (Tức là bị mất nick facebook hoặc Email)

### AVG có thể chạy được trên rất nhiều hệ điều hành khác nhau, [Download phần mềm tại đây](http://congnghe3s.com/download/tai-phan-mem-diet-virus-avg-antivirus-free-2015/)

### Có gì mới trong phiên bản Antivirus 2018

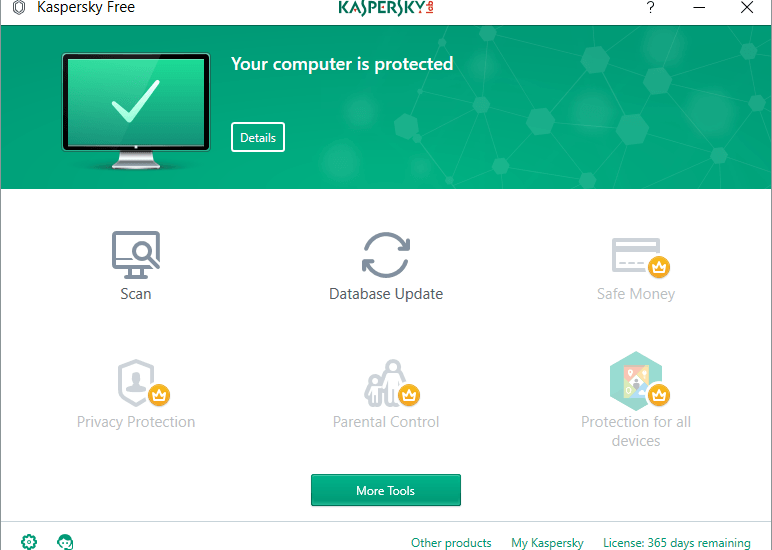
Với giao diện trực quan tuyệt đẹp, thân thiện với người sử dụng. Chỉ 1 lần click là bạn có thể quét virus cho máy tính của mình

Ngoài ra có tính năng mới mà rất nhiều người ngại sử dụng **phần mềm diệt virus** đó là nhiều khi nó không tương thích với game. Nhưng nay Avast Free Antivirus đã khắc phụ được rất nhiều khuyết điểm này. Các thông báo của windows sẽ được tạm dừng để mọi người tiếp tục trò chơi của mình được thoải mái hơn.

Ngoài ra với việc bảo vệ thời gian thực, nó không chỉ kiểm tra được các ứng dụng khi các ứng dụng đó được cài vào. Nó sẽ kiểm tra ngay cả lúc chúng ta sử dụng những ứng dụng để tránh việc tấn công đột ngột qua các ứng dụng trực tuyến.

4. Phần mềm diệt Virus Kaspersky Free

Kaspersky là một hãng **phần mềm diệt virus** rất nổi tiếng rồi. Chắc hẳn ai cũng từng nghe đến hãng bảo mật này. Thay vì trước đây Kaspersky chỉ cho dùng bản dùng thử cho bộ **phần mềm diệt virus** thì giờ đây kaspersky đã cho ra mắt phiên bản miễn phí.



*Kaspersky Antivirus Free*

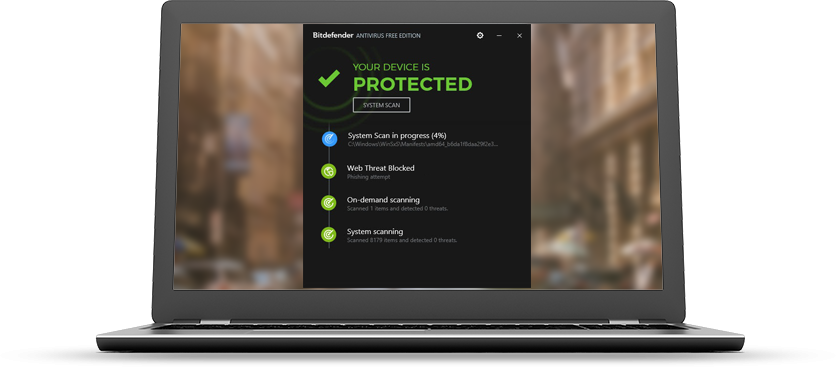
### Những tính năng của Kaspersky Free như sau:

* Bảo vệ máy tính chống lại phần mềm và các trang web độc hại
* Tự động cập nhật khi có bản mới.
* Miễn phí với rất nhiều chức năng cơ bản nhưng cần thiết để máy tính của bạn được an toàn
* Tốc độ quét virus là rất nhanh

Với một người dùng cá nhân thì đây là bộ phần mềm miễn phí rất tốt để bảo vệ được dữ liệu của mình trước sự tấn công của virus

### [Download Kaspersky Free link gốc](http://congnghe3s.com/download/phan-mem-diet-virus-mien-phi-virus-kaspersky-free/)

## 5. Phần mềm diệt virus Bitdefender Antivirus Free



*Bitdefender Antivirus Free*

Nằm cuối trong danh sách giới thiệu của mình là bộ **phần mềm diệt virus Bitdefender Antivirus Free**, theo những người sử dụng trên cnet đánh giá thì Bitdefender free có những ưu điểm như sau:

* Giao diện dễ sử dụng: Giao diện của Bitdefender rất dễ sử dụng, thân thiện với người dùng
* Tính năng tự động quét: Tính năng tự động quyét của Bidefender rất tiện dụng, nó tập trung vào những vùng có nguy cơ cao để quét tránh ảnh hưởng đến tài nguyên của máy tính
* Quét theo thời gian thực: Nó cho phép quét các tập tin, trang web và dữ liệu trong thời gian thực sau đó tiến hành lưu các phần mềm độc hại ở một vị trí nhất định, bảo vệ máy tính của bạn liên tục trong quá trình sử dụng

Nhưng ngoài ra phần mềm này còn có một số những nhược điểm như là không tương thích với một số **phần mềm diệt virus** khác khi cài trên cùng 1 máy tính. Ngoài ra trình cài đặt của phần mềm này cũng rất phức tạp. Vì khi cài đặt mà bạn không để ý bỏ tick chọn ở những mục khời động lại máy tính ở mỗi một bước thì máy tính của bạn sẽ bị khời động lại rất nhiều để có thể cài đặt được phần mềm này thành công trên máy tính của bạn.

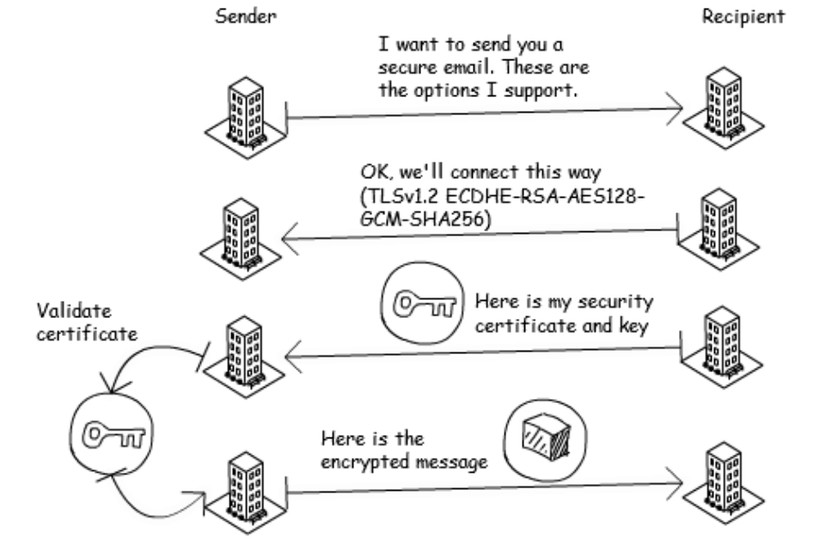
Tuy nhiên với những ưu điểm vượt trội của nó thì đây là một **phần mềm diệt virus miễn phí** rất đáng sử dụng để bảo vệ cho máy tính và dữ liệu cá nhân trong thời kỳ công nghệ 4.0 này.

**3. Các chuẩn bảo mật thư điện tử**

## Transport Layer Security (TLS)

Transport Layer Security (TLS) là một giao thức mã hóa được sử dụng để bảo vệ dữ liệu trong quá trình chuyển tiếp giữa các máy tính. Khi hai máy tính gửi dữ liệu cho nhau, thông tin được mã hóa theo cách mà cả hai đều hiểu. Tùy thuộc vào các quy tắc, một trong hai máy có thể từ chối kết nối nếu không thể tìm thấy một phương pháp mã hóa phù hợp. Trong trao đổi email, máy chủ gửi liên lạc với máy chủ nhận qua kết nối SMTP tiêu chuẩn và sẽ yêu cầu liệu có chấp nhận kết nối TLS an toàn hơn (STARTTLS) hay không. Khi thực hiện điều này, máy chủ gửi chia sẻ một danh sách các giao thức và mật mã mà nó hiểu được. Máy chủ nhận sẽ nhìn vào danh sách và chọn một tùy chọn mà cả hai đều hiểu. Sau đó nó sẽ gửi lại chứng chỉ bảo mật và khóa mã hóa công khai. Máy chủ gửi sẽ kiểm tra chứng chỉ bảo mật hợp lệ, sau đó sử dụng khóa công khai để mã hóa và gửi email. Chỉ máy chủ nhận được có khóa cá nhân có thể giải mã email, vì vậy tin nhắn được gửi được đảm bảo an toàn. Nếu một trong hai máy chủ không thể hỗ trợ kết nối được mã hoá thì chúng sẽ được mặc định kết nối Secure Sockets Layer (SSL) ít an toàn hơn hoặc kết nối không mã hóa. Khi trao đổi email giữa các tổ chức chính phủ, cả hai bên nên nhấn mạnh vào kết nối TLS và từ chối các loại kết nối khác.

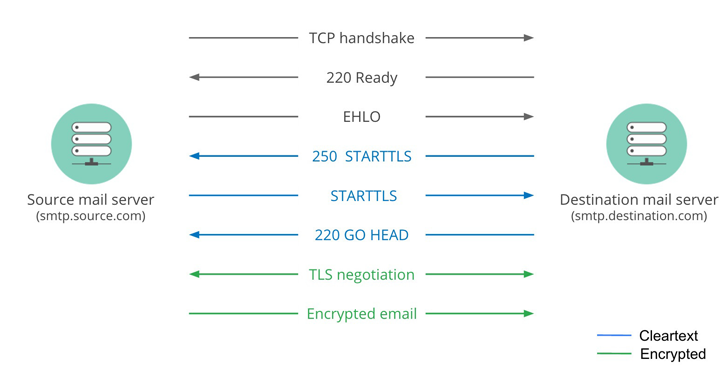
### TLS hoạt động như thế nào ?



Bất kỳ dịch vụ email hiện đại nào đều có thể sử dụng TLS. Trong hầu hết các trường hợp, bạn sẽ có cơ hội lựa chọn sử dụng TLS trên tất cả các kết nối. Điều này có nghĩa là các máy chủ sẽ cố gắng tạo ra một kết nối được mật mã, nhưng nếu họ không thể gửi thì chúng sẽ không được mã hóa. Điều này về cơ bản thì vẫn được , nhưng không đủ để đảm bảo cho việc sử dụng thường xuyên. Để sử dụng thường xuyên, bạn nên tạo ra quy tắc đảm bảo rằng kết nối TLS được thực hiện khi kết nối với một số miền nhất định. Nếu các máy chủ gửi và nhận không thể thống nhất về phương pháp mã hóa, kết nối sẽ bị loại bỏ và không có dữ liệu nào được gửi đi.

TLS cơ hội cần được kích hoạt. Bạn cũng có thể yêu cầu TLS khi bạn biết rằng người gửi hỗ trợ nó. Bằng cách này mọi kết nối không sử dụng nó sẽ tự động từ chối email. Bạn có thể kiểm tra email đã được gửi bằng TLS hay chưa bằng cách xem tiêu đề thư với một phiên bản TLS và mật mã, nhưng những điều này có thể khó hiểu đối với người dùng không phải là dân kỹ thuật. Năm 2002, bằng cách sử dụng kĩ thuật TLS, STARTTLS đã được phát minh ra với vai trò là một bản nâng cấp dành cho kết nối kém bảo mật thành kết nối an toàn. Nhưng STARTTLS cũng rất dễ bị khai thác bằng kỹ thuật tấn công Man-in-the-Middle (MitM) nhằm làm suy yếu khả năng mã hóa.

### Tại sao StartTLS lại không thể đảm bảo an toàn cho Email ?

STARTTLS rất dễ bị khai thác bởi kỹ thuật tấn công MitM nhằm làm khả năng mã hoá bị suy yếu do đó giao thức này không thể đảm bảo cơ chế bảo mật cho thông điệp hay xác thực cho máy chủ. Cơ chế hoạt động của giao thức này như sau:  Khi một client ping đến máy chủ Email, client sẽ hỏi máy chủ Email có hỗ trợ SSL hay không. Tại đây, tin tặc có thể can thiệp vào quá trình thỏa hiệp này và làm Client tin rằng máy chủ Email không hỗ trợ SSL. Điều này đồng nghĩa với việc tin tặc có thể làm suy yếu khả năng mã hoá TLS hoặc thậm chí có thể đọc, sửa được nội dung Email khi Client đã bị thuyết phục và gửi thư trong trạng thái không được mã hoá.

## SMTP Strict Transport Security (SMTP STS)

 Tháng 03/2016, nhóm các kỹ sư đến từ Google, Microsoft, Yahoo, Comcast, LinkedIn và 1&1 Mail đã cùng phát triển một cơ chế bảo mật mới dành cho giao thức truyền tải thư tín đơn giản SMTP (Simple Mail Transfer Protocol).Theo đó, cơ chế mới sẽ cho phép các nhà cung cấp dịch vụ email kiểm soát sâu hơn giao tiếp giữa máy chủ và máy client, tăng cường tính bảo mật và ngăn ngừa tin tặc tấn công.

SMTP Strict Transport Security được thiết kế làm việc cùng với StartTLS để tăng tính bảo mật cho giao thức SMTP nhằm chống lại khả năng làm suy yếu mã hoá từ kỹ thuật tấn công Man-in-the-Middle (MitM) hoặc sửa đổi mail giữa các thiết bị đầu cuối hỗ trợ STARTTLS. SMTP STS hoạt động dựa trên xác nhận chứng chỉ được nhận dạng bởi TLS hoặc DANE TLSA. Chuẩn bảo mật mới này sẽ kiểm tra liệu người nhận email có hỗ trợ SMTP STS hay không và nếu hợp lệ sẽ cập nhật chứng chỉ mã hóa. Email sau đó sẽ được gửi đi. Trong trường hợp email không gửi được, sẽ có thông báo lí do tới người dùng. Cách thức hoạt động của SMTP STS tương tự với HSTS (HTTP Strict Transport Security), nó cũng ngăn ngừa khả năng tấn công hạ cấp bảo mật từ giao thức HTTPS bằng cách lưu đệm lại các chính sách HTTPS của một tên miền ngay trong trình duyệt. Tuy nhiên, nó chỉ an toàn trong trường hợp kết nối đầu tiên từ máy client với máy chủ được thực hiện mà không bị can thiệp. Trong trường hợp kết nối bị can thiệp từ trước, bộ chính sách giả mạo vẫn có thể bị lưu lại.

Mặc dù đã có rất nhiều nỗ lực để áp dụng những chuẩn bảo mật tiên tiến, nhưng trên thực tế việc bảo mật email vẫn còn gặp rất nhiều vấn đề. Vậy người dùng nên có những phương pháp gì để tự mình bảo mật mail một cách tối ưu nhất có thể.

### 1. Không dùng một email cho nhiều dịch vụ

Nếu bạn có nhiều tài khoản email khác nhau, không những chống lại những nguy cơ bị mất cắp mà còn nâng cao hiệu quả của bạn khi sử dụng email trên internet. Mình đoán rằng, bạn sẽ không mấy dễ chịu khi bỗng bắt đầu từ một ngày không đẹp trời nào đó, bạn sẽ nhận được vô số các email quảng cáo mà bạn không quan tâm, đơn giản vì bạn dùng email đó để đăng ký một số dịch vụ và có thể họ dùng nó để bán cho các nhà Email Marketing để tiến hành quảng cáo. Hãy phân chia các email nào dành cho các hoạt động giải trí, công việc, mua sắm, bạn bè…v..v..Và đừng quên, các dịch vụ email hiện nay đều có tính năng thêm tài khoản email phụ, tất nhiên mình đang khuyên bạn nên dùng các email đó để làm email phụ lẫn nhau, vì khi có một trong các tài khoản email đó bị đánh cắp thì bạn vẫn có thể dùng email phụ để khôi phục lại tài khoản.

### 2. Sử dụng mật khẩu thật phức tạp

Đi cùng với nhiều tài khoản email khác nhau là những mật khẩu phức tạp cũng nên khác nhau, tránh việc dùng chung với các mật khẩu email khác hay các dịch vụ khác. Vì nếu bạn luôn sử dụng các mật khẩu giống nhau thì điều đó đồng nghĩa các tài khoản liên quan của bạn sẽ bị mất trắng, bởi nếu hacker đã dùng phương thức mò tìm mật khẩu thủ công thì kiểu gì họ lại không thử gõ lại mật khẩu mà họ đã biết.

### 3. Đề phòng với các mánh khóe lừa đảo

Hãy cảnh giác cao độ với các email yêu cầu cung cấp thông tin cá nhân và nên kiểm tra rõ ràng từ địa chỉ người gửi, đến địa chỉ website mà bạn vừa nhấp vào. Chẳng hạn như giả mạo các website uy tín để gửi các email khuyến mãi hấp dẫn và khi bạn nhấp vào nó sẽ yêu cầu bạn nhập email và mật khẩu, và kể từ đó các mật khẩu của bạn sẽ rơi vào tay các kẻ lừa đảo.

### 4. Đừng bao giờ nhấp vào liên kết trong email

Cũng là một kiểu lừa đảo tinh vi khác, họ sẽ mạo danh các nhà dịch vụ uy tín để gửi các thông tin hấp dẫn mà bạn cần phải nhấp vào một liên kết nào đó trong email. Tốt nhất là đừng bao giờ click vào nó bởi nguy cơ 99% là lừa đảo , 1% ngoại lệ còn lại là trừ khi bạn đang mong chờ một email nào đó ví dụ như kích hoạt tài khoản diễn đàn, xác nhận một trò chơi nào đó. Còn khi bạn nhận email từ các dịch vụ quan trọng như ngân hàng, nhà cung cấp hosting, hóa đơn thanh toán…v..v..mà bạn sợ bỏ qua nó thì nên nhập lại liên kết đó bằng tay không bao giờ nhấp hay copy các liên kết đó và dán vào trình duyệt.

### 5. Không mở các file đính kèm không cần thiết

File đính kèm luôn là một mục tiêu hàng đầu cho các kẻ gian gửi gắm những “thông điệp” mang tính chất lừa đảo. Nếu không phải bạn đang đợi các tập tin quan trọng từ bạn bè, gia đình hay đồng nghiệp thì đừng bao giờ mở nó khi không thật sự cần thiết. Rất có thể đằng sau những tập tin hình ảnh .JPG là những tập tin .EXE được nguy trang khéo léo, và khi bạn tải về và mở nó ra, bạn đã có trên tay một chú virus thật dễ thương.

### 6. Quét virus và malware sau khi tải tập tin về từ email

Nếu bạn quyết định tải một tập tin từ email khác về mà cho rằng nó vô tội thì cũng đừng quên hãy quét nó qua một lần bằng các phần mềm diệt virus uy tín. Cũng trên các phần mềm Internet Security hiện nay đều có tính năng scan và kiểm tra vius trong email, vì thế đừng bao giờ đưa nó vào quên lãng nếu không muốn phải hối hận sau này.

### 7. Tránh xa các mạng Wi-Fi công cộng

Các mạng Wi-Fi công cộng cực kỳ nguy hiểm và kém an toàn. Có một số công cụ có thể đe dọa đến an ninh mạng trên Wi-Fi được gọi là “Network Sniffers” được chạy ngấm ngầm trên các thiết bị của những kẻ gian. Các Sniffers sẽ có thể giám sát mọi dữ liệu được truyền đi thông qua một mạng không dây được định sẵn, và ở đó các thông tin sẽ được phân tích ra các thông tin nhạy cảm mặc dù nó đã được mã hóa. Nó cùng nghĩa với việc tên đăng nhập và mật khẩu của bạn có thể bị giám sát và hiển thị đầy đủ trong kho dữ liệu của các hacker.

### 8. Sử dụng 2 lớp mật khẩu bảo mật

Nếu bạn đang sử dụng Gmail thì đừng bỏ qua một tính năng là tạo 2 lớp bảo mật cho tài khoản khi đăng nhập. Ở lớp thứ nhất, bạn sẽ nhập mật khẩu của mình như thường lệ, và ở bước thứ hai, họ sẽ yêu cầu bạn nhập một mã số bảo mật được gửi trực tiếp qua điện thoại di động sau khi bạn vượt qua lớp thứ nhất. Như vậy có nghĩa là cho dù hacker có trong tay tài khoản và mật khẩu của bạn thì cũng không làm được gì trừ khi họ có luôn cái sim điện thoại của bạn. Nếu bạn chưa kích hoạt tính năng này thì có thể xemhướng dẫn kích hoạt 2 lớp bảo mật trên trang hỗ trợ của Google.

**Câu 4. An toàn dữ liệu thanh toán điện tử.**

Giải pháp an toàn trong thanh toán điện tửNhư đã giới thiệu ở trên, cách tốt nhất bảo đảm an toàn trong thanh toán điện tử là mã hóa các thông tin cần được truyền đi trên mạng. Hiện nay có nhiều giao thức được sử dụng cho phép thực hiện giao dịch trong không gian ảo. Bản chất của giao dịch cũng chỉ là sự chuyển tiền từ tay người này qua người khác. Trong phần này chúng ta sẽ xem xét hai giao thức mở cho phép thực hiện giao dịch an toàn, đó là SSL và SET.1. Giao thức tầng cắm an toàn (Secure Sockets Layer – SSL)Giao thức SSL được thiết kế bởi Nestcape như là một phương pháp bảo đảm sự an toàn của kết nối khách (client) – chủ (server) trên môi trường Internet. SSL là công nghệ để mã hóa việc truyền dữ liệu giữa trình duyệt web và máy chủ web. Công nghệ này được sử dụng thường xuyên bởi các trang web ngân hàng trực tuyến và trang web thương mại điện tử. Trang web khác cũng có thể triển khai SSL dưới hình thức hạn chế hơn -- ví dụ: để giúp bảo vệ mật khẩu của bạn khi nhập thông tin đăng nhập của bạn. Địa chỉ web được bảo mật bằng SSL bắt đầu với https: t hay vì http: nên các điều khoản thường được sử dụng thay thế cho nhau.Cơ Chế Hoạt Động Của SSLVề cơ bản, giao thức SSL hoạt động ngay dưới các giao thức ứng dụng (như HTTP, SMTP,Telnet, FTP, Gopher và NNTP) và nằm trên giao thức mạng TCP/IP. Điều đó cho phép SSL vận hành độc lập đối với các giao thức ứng dụng mạng. SSL sử dụng phương pháp mã hóa khóa công khai đã giới thiệu ở trên, với thuật toán RAS dùng để mã hóa. SSL cho phép: - Client và server nhận dạng lẫn nhau.- Sử dụng chứng thực số để chứng thực tính toàn vẹn.- Mã hóa toàn bộ thông tin để đảm bảo tính bí mật. Để làm được điều này cần có một máy chủ bảo mật, đó là lý do tại sao bạn thường nhận được thông báo kiểu này:Các máy chủ bảo mật thường có chuỗi HTTPS và hình chiếc khóa trong URL thay vì HTTP như bình thường.Quá trình bạn bắt đầu một phiên làm việc với một máy chủ web dưới sự bảo mật của SSL được gọi là “quá trình bắt tay”. Một quá trình bắt tay bao gồm:- Trình duyệt và server quyết định cấp độ và cách thức mã hóa dùng cho phiên làm việc.- Trình duyệt và server tạo và chia sẻ chìa khóa dùng để mã hóa.- Trình duyệt yêu cầu và nhận chứng thực số từ server (không bắt buộc).- Server yêu cầu và nhận chứng thực số từ trình duyệt (không bắt buộc).Sau khi quá trình bắt tay kết thúc, bạn hoàn thành giao dịch. Chỉ cần phiên làm việc chưa kết thúc thì mọi dữ liệu truyền đi giữa trình duyệt và server đều được mã hóa. Khi phiên làm việc hoàn thành, trình chủ bảo mật sẽ chuyển bạn về trình chủ không bảo mật.SSL an toàn đến đâu?Hầu hết chúng ta không quan tâm tới việc SSL hoạt động như thế nào, chúng ta chỉ muốn biết nó có thực sự hoạt động hay không. Nếu nó giữ thông tin thẻ tín dụng của bạn an toàn thì không có gì phải phàn nàn. Tất nhiên, mã hóa sử dụng trong SSL có thể bị phá vỡ nhưng rất tốn kém. Trong hầu hết các ứng dụng, SSL vẫn được coi là giải pháp hàng đẩu để bảo vệ thông tin thẻ tín dụng khi giao dịch trực tuyến. Hơn nữa, SSL có thể được phát triển, đặc biệt nếu Nestcape và Microsoft được chính phủ Mỹ cho phép sử dụng những phương pháp mã hóa mạnh hơn.

**5. An toàn Website**

1. Dùng mật khẩu mạnh

dung mat khau manh de bao ve may tinh

Thoạt nghe đến đây, SecurityBox chắc chắn rằng các bạn đọc nghĩ điều này là khá bình thường. Tuy nhiên việc sử dụng một mật khẩu mạnh chính là giải pháp giúp đảm bảo sự an toàn trong bảo mật hệ thống website cũng như máy chủ. Mật khẩu cần được thay đổi thường xuyên và định kỳ, khoảng 1 tháng 1 lần.

Theo SecurityBox, một mật khẩu mạnh, cầnphải đáp ứng được những tiêu chí sau đây. Mật khẩu phải bao gồm chữ và số cùng với các ký tự đặc biệt, tuy vậy cần phải dễ nhớ. Thứ 2 đó là sử dụng nhiều mật khẩu khác nhau, không nên dùng một mật khẩu cho nhiều loại tài khoản khác nhau. Bởi vì nếu một khi bị lộ ra toàn bộ các tài khoản cũng sẽ bị lộ ra.

Để kiểm tra xem website của bạn có bảo mật, an toàn 100% hay không, SecurityBox khuyên bạn nên dùng một số công cụ kiểm tra lỗ hổng website tại bài viết này: 20 công cụ test bảo mật website hiệu quả nhất

Thường xuyên cập nhật

Để có thể nâng cao mức độ bảo mật hệ thống website, người quản trị website phải cập nhật thường xuyên định kỳ đối với website của mình. Đặc biệt là phải theo dõi những phiên bản mới nhất nếu như bạn đang dùng những mã nguồn mở. Việc này sẽ làm giảm nguy cơ từ những cuộc tấn công vào website của bạn với mục đích khai thác dữ thông tin, thay đổi quyền quản trị, thay đổi mật khẩu..

Luôn phải tạo các bản sao lưu

sao lưu du lieu

Để bảo mật hệ thống dữ liệu, file, máy tính bạn cần sao lưu dữ liệu thường xuyên

Một nguyên tắc bảo mật hệ thống website cực kỳ quan trọng đó là luôn phải tạo một bản sao lưu toàn bộ nội dung vào thời điểm hệ thống của bạn chưa bị tấn công hay bị nhiễm mã độc. Việc này nhằm mục đích giúp bạn khôi phục lại dữ liệu hệ thống của bạn khi có sự cố xảy ra , ngoài ra việc này còn giúp tiết kiệm thời gian và công sức rất nhiều khi khôi phục hệ thống của bạn. Tạo một bản sao định kỳ sẽ giúp ích trong việc giải quyết những vấn đề bất chợt xảy ra như máy chủ hoặc website của bạn bị nhiễm mã độc.

>> Sao lưu, cập nhật win, bản vá mới nhưng chưa đủ, quan trọng nhất là bạn cần nắm được những lỗi bảo mật website đầy đủ mới được SecurityBox cập nhật đầu năm 2017.

Thường xuyên quét các tập tin

Đây là một thao tác đơn giản mà hữu ích để bảo mật hệ thống website của bạn. Việc thường xuyên quét những tập tin ở trên máy chủ sẽ kịp thời phát hiện những tập tin bị nhiễm độc. Hãy nhớ quét tập tin định kỳ kể cả khi không có dấu hiệu nhiễm độc nào được phát hiện.

Mức độ bảo mật của máy chủ cần phải được tăng cường

Nếu như bạn sở hữu một hệ thống máy chủ thì người quản trị cần phải chú ý đến cấu hình máy để có thể đảm bảo mức độ an toàn cao nhất có thể. Để tăng cường bảo mật máy chủ cần làm những việc sau. Loại bỏ tất cả các phần mềm không sử dụng. Vô hiệu hóa tất cả các dịch vụ và module không cần thiết. Thiết lập chính sách phù hợp cho người dùng và các nhóm. Thiết lập quyền truy cập,hạn chế truy cập vào các tập tin và thư mục nhất định. Vô hiệu hóa việc duyệt thư mục trực tiếp. Thu thập các tập tin ghi nhận hoạt động, thường xuyên kiểm tra các hoạt động đáng ngờ. Sử dụng mã hóa và các giao thức an toàn.

Trên đây, SecurityBox vừa chia sẻ với bạn 5 bước bảo mật hệ thống website cơ bản nhất Nếu bạn không hiểu chỗ nào, hoặc cần tư vấn, hỗ trợ hãy chat với chúng tôi qua fanpage facebook: SecurityBox. Thân !