Vấn đề về bảo mật trên mạng Internet

Bởi:

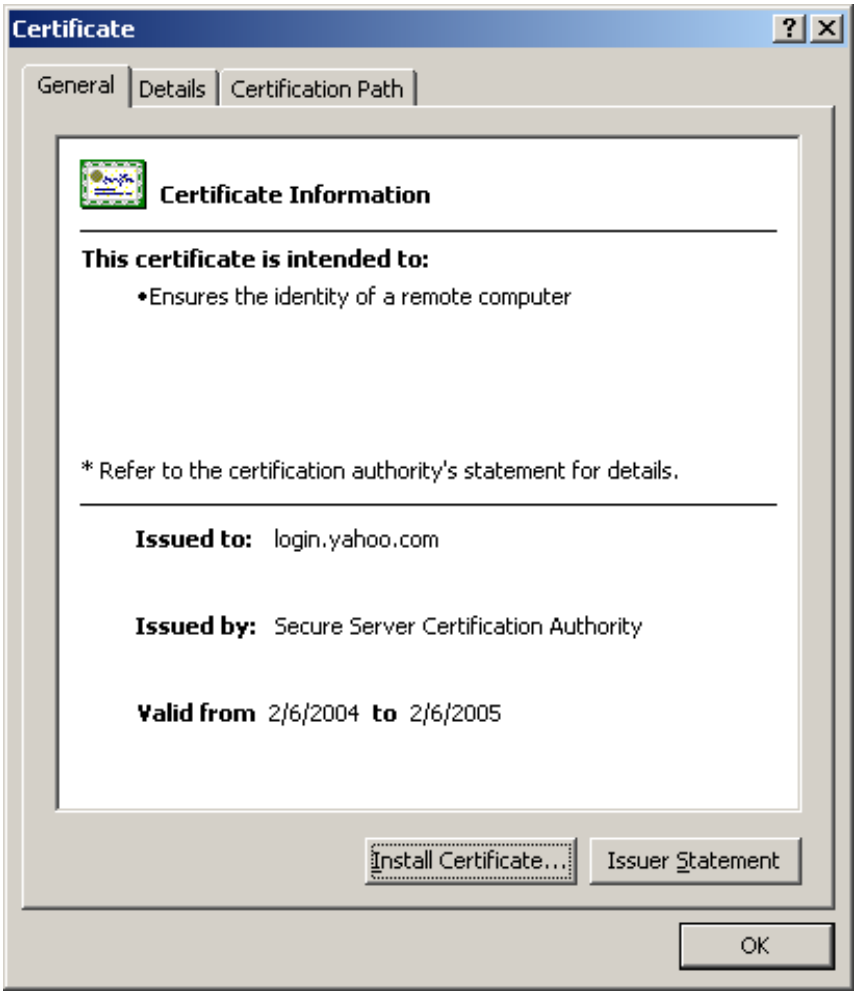
Đỗ Ngọc Minh

Thế nào là một website được bảo vệ

- Một website được bảo vệ là một website chỉ cho phép truy nhập có giới hạn, muốn sử dụng các dịch vụ hoặc xem thông tin, phải đăng nhập bằng tên và mật khẩu. Nếu bạn không được cấp quyền hoặc bạn đã được cấp tên đăng nhập nhưng mật khẩu gõ vào không chính xác thì bạn sẽ không thể truy nhập được nội dung của website đó.
- Rất nhiều công ty hoặc cơ quan tổ chức sử dụng cách này để cho phép thông tin có thể được phân phối rộng rãi, nhưng là phân phối cho đúng các đối tượng quan tâm hoặc các đối tượng trong ngành. Các ví dụ khác là những website của các công ty thương mại muốn bán các thông tin, website của các tổng công ty mà chỉ cho phép các công ty thành viên truy xuất, người ngoài không được truy xuất vào...

Tìm hiểu về chứng nhận số

- Chứng nhận số được sử dụng để mã hoá các thông tin và truyền đi trên Internet. Một chứng nhận số có thể sử dụng để tạo ra một chữ ký số cho một email, chữ ký này đảm bảo việc nhận biết người gửi, nó cũng đảm bảo nội dung thư không bị xem hoặc thay đổi trái phép trong khi nó được truyền đi.
- Chứng nhận số có thể mua tại một tổ chức có chức năng chứng thực ví dụ như www.verisign.com, ở đó sẽ có các hệ thống chứng thực thông tin cho bạn.
- Các chứng nhận số thường được sử dụng bởi các website mua bán hàng trên Internet hoặc các trang cho phép thu nhận thông tin cá nhân người dùng nhằm mã hoá các thông tin về tài khoản của bạn sao cho chúng không bị thâm nhập khi truyền qua mạng Internet. Ví dụ bạn có thể truy xuất vào địa chỉ https://mail.yahoo.com, là trang web đã được sử dụng chứng nhận số. Sau đó, để xem thông tin về chứng nhận số, bạn có thể nhấn chuột vào biểu tượng chiếc khóa ở trên thanh trạng thái của trình duyệt, bạn có thể thấy được các thông tin như sau:



Thông tin về chứng nhận số của website https://mail.yahoo.com

Tìm hiểu về mã hoá

- Mã hoá là cách thức để "che dấu" thông tin. Mã hóa được sử dụng để tăng cường tính bảo mật cho các thông điệp mà ở đó chỉ có người được gửi mới có thể đọc được thông điệp đó.
- Có nhiều cách để thực hiện việc mã hoá, cả bằng phần cứng và phần mềm. Ví dụ về một cách mã hoá như sau: chuỗi ký tự bình thường là *Hello*, nhưng với thuật toán mã hoá dịch chuyển 2 ký tự, chuỗi trên trở thành *Jgnnq* (H -dịch 2 chữ - thành J, e - dịch 2 chữ - thành g…) và nếu ai đó lấy được chuỗi *Jgnnq* mà không biết thuật toán mã hoá thì sẽ không biết rằng đó là chuỗi *Hello*.
- Mã hóa có nhiều mức độ, các mức độ đó thường được miêu tả bằng số bit sử dụng trong thuật toán mã, như thuật toán mã hoá 32-bit, 64-bit, 128-bit…Sử dụng càng nhiều bit để mã hoá, hệ thống sẽ càng được bảo mật hơn.

Nguy cơ nhiễm virút khi tải về các tệp từ Internet

- Tài nguyên trên Internet rất phong phú và đa dạng và nhu cầu tải về sử dụng nguồn tài nguyên này là nhu cầu của mọi người. Trong kho tàng khổng lồ này có rất nhiều tài nguyên bổ ích nhưng cũng có rất nhiều các nguy cơ tiềm ẩn. Nếu bạn tải về bất kỳ một tài nguyên gì từ Web, một tệp tin tài liệu, một tệp tin âm thanh, một chương trình tiện ích… thì khả năng tệp tin đó đã bị nhiễm một loại virút máy tính nào đó là hoàn toàn có thể.
- Để tự bảo vệ mình chống lại virút, bạn nên cài đặt một phần mềm chống virút (ví dụ như Norton Anti-Virus). Phần mềm này sẽ kiểm tra các tệp tin bạn mới tải về và thông báo cho bạn biết tệp tin đó có chứa virút không. Để giúp cho phần mềm diệt virút luôn có khả năng phát hiện virút mới, bạn phải cập nhật thường xuyên các phần mềm chống virút, để từ đó máy tính có khả năng chống được các loại virút mới xuất hiện.

Một số vấn đề rắc rối có thể xảy ra khi người dùng tham gia vào Internet .

- Vấn đề thư rác (spam mail): Bạn phải suy nghĩ cẩn thận trước khi quyết gõ địa chỉ email của bạn vào các form đăng ký trong các website mà bạn không quen biết. Có thể sau đó bạn sẽ nhận được những lá thư chào hàng hoặc các bức thư quảng cáo từ những website đó. Tồi tệ hơn, địa chỉ email của bạn có thể sẽ bị chuyển đến các công ty chuyên bán các địa chỉ email để quảng cáo, sau đó bạn sẽ liên tục nhận được những lá thư spam không mời mà đến.
- Sự lừa gạt: Bạn nên chú rằng đừng bao giờ chỉ ra các thông tin cụ thể về thẻ tín dụng của bạn cho bất cứ ai hay bất cứ công ty nào trừ khi bạn biết rằng bạn đang trao đổi buôn bán với một tổ chức có uy tín. Nếu không, có thể bạn sẽ thấy rằng những mặt hàng mà bạn đăng ký sẽ không bao giờ được chuyển tới, hoặc tệ hơn thẻ tín dụng của bạn sẽ được sử dụng một cách phi pháp. Ví dụ, bạn vào một trang web nào đó mà bạn chưa chắc chắn về độ tin cậy lắm, nhưng trong trang web đó có trưng bày rất nhiều hàng hoá với giá cả phải chăng. Nếu ở trong thế giới thực, bạn có thể tin tưởng được, nhưng đây là thế giới Internet, nơi mà *những gian hàng như thế có thể lập nên hết sức dễ dàng*. Trong trường hợp đó, bạn không nên đưa thông tin về thẻ tín dụng của mình vội mà nên xem xét tư cách bán hàng của công ty trên trước đã.

Thuật ngữ tường lửa (firewall)

- Tường lửa là một hệ thống bao gồm cả phần cứng và phần mềm có mục đích chống lại sự xâm nhập trái phép từ Internet. Thông thường, tường lửa được đặt tại khu vực ranh giới giữa mạng nội bộ của công ty và bên ngoài. Bất kỳ một thông tin nào muốn đi ra khỏi công ty hoặc từ ngoài chuyển vào đều có sự ngăn chặn hoặc kiểm soát từ tường lửa.

- Trong các cơ quan hoặc tổ chức lớn, hệ thống tường lửa được thiết lập và vận hành bởi đội ngũ các chuyên viên công nghệ thông tin. Trong hầu hết các trường hợp, bạn không cần phải quan tâm đến sự tồn tại của hệ thống tường lửa này. Là một người sử dụng, thời điểm duy nhất mà bạn phải quan tâm đến tường lửa là khi bạn truy nhập vào một số site nào đó, bạn cần nhớ các thông số cấu hình để bạn có thể vượt qua tường lửa hoặc nếu bạn sử dụng giao thức chuyển tệp tin FTP thì đôi khi tường lửa sẽ không hỗ trợ dịch vụ này.