NHỮNG CÁI BẪY TỪ CÁC ĐIỂM TRUY CẬP INTERNET KHÔNG DÂY

Bạn vào một quán - điểm truy cập internet không dây để vừa thưởng thức cà phê và vừa o-nline bằng máy tính xách tay của mình. Bạn kết nối vào mạng không dây và bắt đầu thực hiện các giao dịch thông qua ngân hàng hay mua

Bạn vào một quán - điểm truy cập internet không dây để vừa thưởng thức cà phê và vừa o-nline bằng máy tính xách tay của mình. Bạn kết nối vào mạng không dây và bắt đầu thực hiện các giao dịch thông qua ngân hàng hay mua một món hàng nào đó trên mạng… Với tư cách là người dùng đầu cuối, bạn cảm thấy an toàn khi thấy biểu tượng hình chiếc khóa bên dưới trình duyệt web Internet Explorer. Các thông tin của bạn, bao gồm username, password, thông tin tài khoản, thẻ tín dụng… được mã hóa ở chế độ 128 bit. Thực tế, việc giao dịch này có thật sự an toàn không? Đối với giao dịch qua ngân hàng hay mua hàng trên mạng thì nói chung là khá an toàn, đặc biệt khi nó được thực hiện thông qua SSL (Secure Sockets Layer). Secure Sockets Layer là một giao thức được phát triển bởi hãng Netscape nhằm giúp truyền tải các tài liệu có tính riêng tư thông qua mạng internet. SSL sử dụng một hệ thống mã hóa với hai khóa để mã hóa dữ liệu: một khóa công cộng để mọi người được biết và một khóa riêng tư - hay còn gọi là khóa bí mật - mà chỉ có người nhận thông tin mới biết được. Cả Netscape Navigator và Internet Explorer đều hỗ trợ SSL, nhiều trang web sử dụng giao thức này để tiếp nhận các thông tin mật từ người dùng như số tài khoản, thẻ tín dụng.... Theo quy ước thì các URL cần một giao dịch an toàn sẽ bắt đầu bằng chữ https: để thay cho http:. Tuy nhiên, bạn có thể không nhận ra được một hacker có thể đánh cắp thông tin khi bạn thực hiện giao dịch qua ngân hàng hay thông tin trên thẻ tín dụng của bạn. Điều này xảy ra khi bạn không giao dịch trực tiếp với đối tượng cần thiết (như ngân hàng) mà lại giao dịch với một trung gian khác (hacker), hay còn gọi là Man-in-the-middle.. Việc đánh cắp thực hiện như thế nào ? Kẻ cắp sẽ vào cùng một quán cà phê và cùng kết nối vào mạng Wi-Fi với bạn. Hắn ta sẽ cho chạy hàng loạt các chương trình để kết nối các dữ liệu từ máy tính của người bị hại vào máy tính của mình. Hắn ta tiếp tục cho chạy hàng loạt các chương trình khác để đánh hơi các dữ liệu, nó hoạt động như là một SSL Certificate Server và trở thành giao dịch trung gian (Man-in-the-middle) giữa người bị hại với giao dịch mà họ cần. Hình 1 có thể giúp bạn hiểu rõ hơn. Một khái niệm quan trọng mà người giao dịch nên biết là các chứng thực (certificate) được dùng để thiết lập một giao dịch an toàn. Một chứng thực tốt đồng nghĩa với việc kết nối trực tiếp tới nơi cần giao dịch một cách an toàn. Khi đó tất cả các dữ liệu mà bạn cần giao dịch sẽ được mã hóa bằng trình duyệt web bạn đang sử dụng, sau đó nó sẽ được gửi trực tiếp tới nơi cần giao dịch, tiếp theo nó sẽ được giải mã để sử dụng. Khi thực hiện theo cách này thì cho dù hacker có được các thông tin về dữ liệu của bạn thì hắn ta cũng khó có thể giải mã được. Tuy nhiên, thật tệ hại nếu như người bị hại nhận được một chứng thực giả mạo được gửi tới từ hacker, khi đó người bị hại không kết nối tới ngân hàng cần giao dịch mà lại kết nối tới máy tính của hacker. Trong trường hợp này thông tin sẽ được truyền từ trình duyệt web của người bị hại tới máy tính của hacker và hắn ta sẽ chộp lấy các thông tin đó. Do chứng thực giả mạo đó được tạo ra từ hacker cho nên hắn sẽ dễ dàng mã hóa ngược lại để lấy các thông tin mà người bị hại gửi đi. Phòng tránh Khi hacker đưa ra các chứng thực giả mạo để thay thế các chứng thực đúng thì hầu hết những người sử dụng đều "gật đầu". Sau đây là những ví dụ do trung tâm Security Alert đưa ra mà người sử dụng có thể nhận được. Hầu hết những người không am hiểu tường tận sẽ chọn "Yes"... khi xuất hiện cửa sổ như hình 2 và khi đó họ đã tự làm khó cho mình: Bằng cách nhấp "Yes", bạn đã tự đưa mình vào bẫy của hacker. Tuy nhiên nếu nhấp vào nút "View Certificate" thì bạn có thể thấy vấn đề. Sau đây là

một ví dụ về chứng thực giả và chứng thực thật để bạn so sánh: Do đó, để tránh bị đánh cắp thông tin về tài khoản thẻ tín dụng thì bạn cần lưu ý một số điều sau đây: * Nên vào trang web Security Alert để đọc những hướng dẫn cần thiết về cách phòng tránh bị đánh cắp thông tin trên thẻ tín dụng. * Nên sử dụng các password chỉ một lần, sau đó thì nên đổi cái khác để tránh bị đánh cắp password. * Khi sử dụng SSL VNP thì nên sử dụng các chức năng nâng cao. * Nên sử dụng Firewall khi sử dụng internet không dây ở các nơi công công.