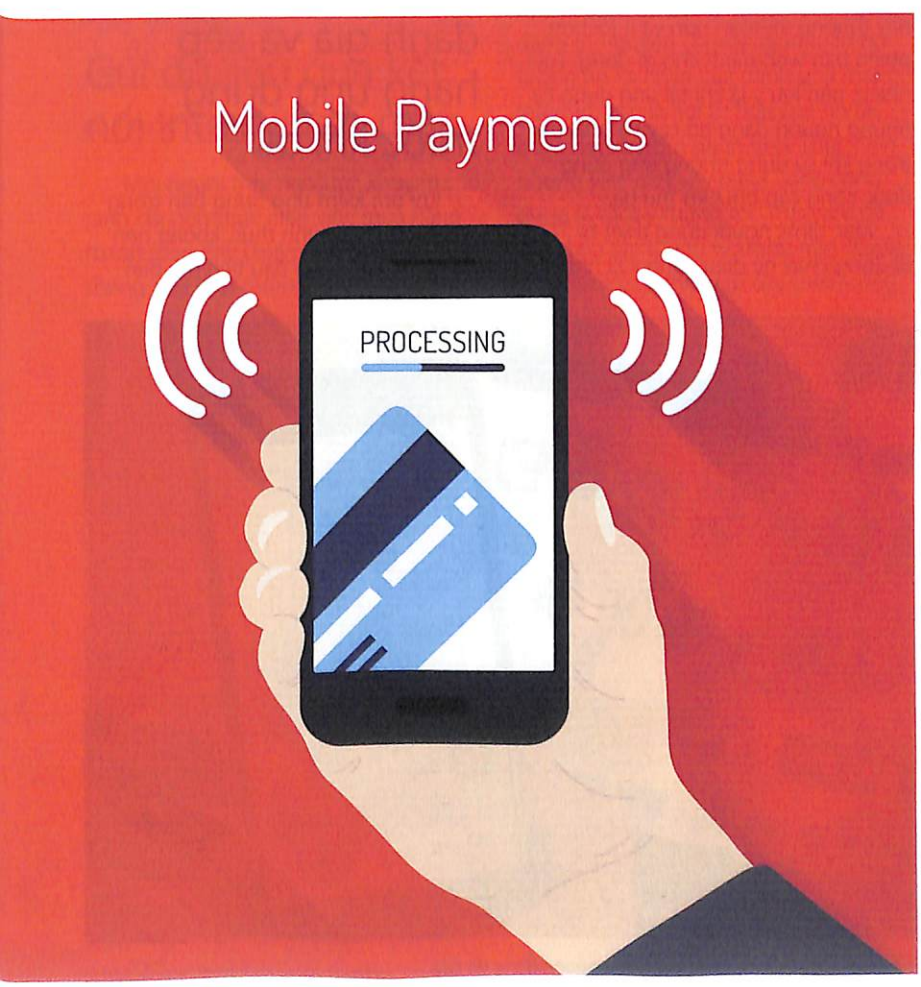
5 bước an toàn khi thanh toán qua di động

Đặt mật khẩu thiết bị, tải ứng dụng từ nguồn tin cậy, gửi dữ liệu qua kết nối an toàn... là những bước cần làm để bảo vệ thông tin khi thực hiện thanh toán di động.

Thanh toán di động (*mobile payment*) đang trở thành một xu hướng tất yếu trong thời đại công nghệ ngày nay, một kênh phân phối dịch vụ hiệu quả và tiện lợi nhằm đáp ứng nhu cầu mua sắm trực tuyến của khách hàng mọi lúc mọi nơi. Khách hàng đang dần chuyển từ giao dịch trên nền tảng máy tính truyền thống qua mạng Internet sang giao dịch trên điện thoại di động.

Tuy nhiên, song song với việc phát triển của các dịch vụ mobile payment là nỗi lo về vấn đề bảo mật khi mua sắm trực tuyến bằng di động. Cụ thể hơn, người dùng phải làm như thế nào để được bảo vệ an toàn khi mua hàng trên thiết bị di động? Bài viết sẽ cung cấp một số lời khuyên và ý tưởng về việc mua hàng trên smartphone và tablet, vốn là những thiết bị có thể kém an toàn hơn so với máy tính truyền thống.



Bảo vệ thiết bị di động bằng mật khẩu

Một vài người dùng cảm thấy thực sự không thoải mái khi phải thiết lập khóa điện thoại hay máy tính bảng bằng mật khẩu. Nếu bạn là người hay đãng trí bỏ quên thiết bị di động của mình mọi lúc mọi nơi thì cài đặt khóa mật khẩu chính là một trong những giải pháp an toàn nhằm tránh người khác có thể tò mò vọc vạch và vô tình lợi dụng chúng để mua sắm trực tuyến.

Tất nhiên việc đặt mật khẩu thiết bị sẽ không bảo vệ bạn tránh được tình trạng kẻ xấu rình mò các gói dữ liệu trên đường truyền Internet, nhưng được xem là cách tốt nhất chống lại ai đó đoạt được quyền truy cập trực tiếp khi cầm chiếc điện thoại của bạn. Điều này có nghĩa là bất cứ khi nào ai đó mở iPhone hoặc điện thoại Android của bạn, nó sẽ yêu cầu một mật mã trước khi mở khóa. Đây là một giải pháp tuyệt với nếu bạn là người thường xuyên di chuyển đi công tác hay đi du lịch với một thiết bị được bảo vệ an toàn hơn bên mình.

Việc thất lạc điện thoại hay máy tính bảng là điều luôn có thể xảy ra.

Đặt mật khẩu thiết bị là một trong những cách đơn giản nhất để bảo vệ các giao dịch trực tuyến.

Tình huống sẽ nguy hiểm hơn nếu thiết bị đang được cấp quyền truy cập trực tiếp vào tài khoản ngân hàng và giỏ hàng trực tuyến của bạn. Về mặt kỹ thuật, bạn có thể khóa vài ứng dụng cụ thể nhưng điều này thường phức tạp hơn là hữu dụng so với việc đặt mật khẩu để khóa việc truy xuất toàn bộ thiết bị.

Tải ứng dụng từ những nguồn đáng tin cậy

Thông thường, các công ty bán hàng trực tuyến luôn có trang web (cả phiên bản để bàn lẫn di động) để bạn có thể truy cập bằng trình duyệt và lựa chọn mua sắm. Khi sử dụng giải pháp này, bạn cần phải chuyển dữ liệu trên web thông qua trình duyệt và điều đó dễ dẫn đến nguy cơ rò rỉ thông tin trong đường truyền.

Bên cạnh đó, nhiều dịch vụ còn cung cấp một ứng dụng di động riêng để người dùng sử dụng trực tiếp trên smartphone hay tablet. Khi chọn giải pháp này, bạn hoàn toàn bị giới hạn vào giao diện người dùng phía máy chủ (*backend*) và đây thường được xem là một phương pháp an toàn hơn so với truy cập trang web qua trình duyệt.

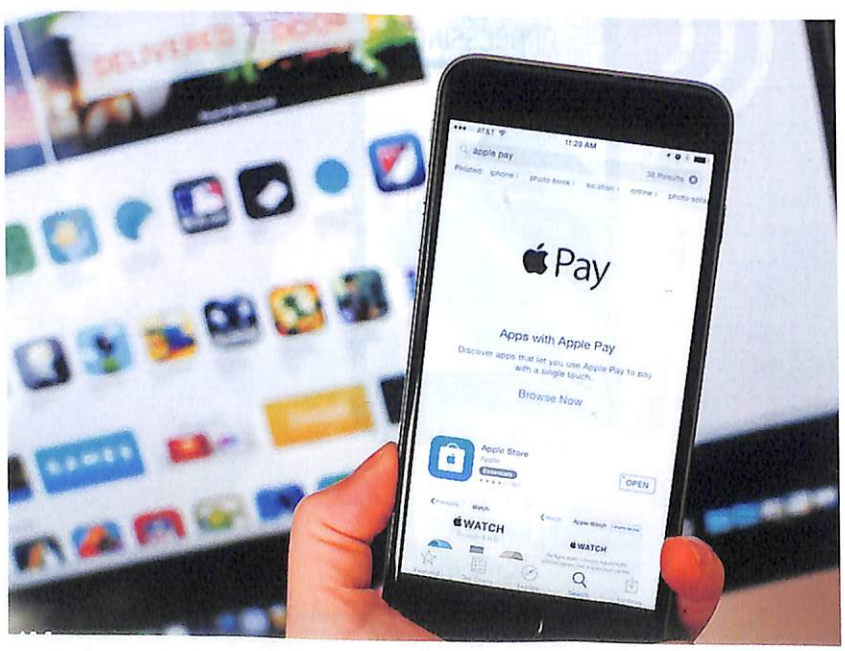
Vì vậy, nếu bạn thường xuyên mua sắm trên các dịch vụ bán hàng trực tuyến bằng chiếc điện thoại của mình, đầu tiên hãy kiểm tra các cửa hàng App Store chính thức và xem có ứng dụng chính hãng hay không. Các ứng dụng này thường an toàn hơn và ít lỗi hơn phiên bản web dành cho di động. Tuy nhiên, nên lưu ý là chỉ tải ứng dụng từ những nguồn đáng tin cậy và phải cẩn trọng khi sử dụng những ứng dụng được cung cấp bởi bên thứ ba.

Mặc định, người dùng thiết bị di động chạy hệ điều hành iOS như iPhone và iPad đều bị buộc phải tải ứng dụng từ một nguồn chính thức duy nhất, đó là cửa hàng trực tuyến App Store của Apple vốn được xem là nơi được kiểm duyệt nghiêm ngặt trước khi xuất hiện công khai. Tuy nhiên, người dùng iOS vẫn có thể "vượt rào" bằng cách bẻ khóa (*jailbreak*) thiết bị của họ để tải ứng dụng từ các nguồn không chính thức khác như Cydia App Store.

Trong khi đó, Google Play Store không phải là nguồn cung cấp ứng dụng duy nhất cho thiết bị Android vì người dùng vẫn còn nhiều cách khác để cài đặt ứng dụng trên hệ điều hành này. Tuy nhiên, nên lưu ý rằng chỉ tải và cài đặt ứng dụng từ những nguồn đáng tin cậy. Dù gì đi nữa, việc tải ứng dụng từ bên thứ ba ngoài các cửa hàng chính thức của Google hay Apple là một quyết định rất mạo hiểm.

Kiểm tra các mục đánh giá và xếp hạng ứng dụng trước khi tải

Khi tìm kiếm ứng dụng bên trong các App Store chính thức, không nên tải về các tùy chọn đầu tiên mà bạn



Chỉ nên chọn tải ứng dụng từ những nguồn đáng tin cậy.

nhìn thấy. Đôi khi ứng dụng đó có thể được phát triển bởi một bên thứ ba và những nhà phát triển ứng dụng này không chính thức liên kết với các trang web bán hàng trực tuyến. Không ai biết được dữ liệu thông tin cá nhân và thông tin thẻ thanh toán mà bạn cung cấp trong ứng dụng sẽ đi về đâu. Đây là một hiện tượng rất hiếm nhưng bạn cũng cần cảnh giác khi tìm thấy.

Trong danh sách kết quả tìm kiếm, bạn sẽ thấy mỗi ứng dụng có phần đánh giá xếp hạng. Biểu đồ dao động từ 0,5 sao cho đến đầy đủ 5 sao. Cùng với việc người dùng đánh giá thực tế, bạn cũng có thể nhìn thấy bao nhiêu người đã bình chọn và một số ý kiến của họ. Nội dung phần ý kiến thường hữu ích hơn việc xếp hạng sao bởi vì bạn có thể nhận được những thông tin phản hồi thực tế của người đã từng dùng qua ứng dụng. Đừng ngần ngại việc lướt qua phần đánh giá ứng dụng trước khi tải về.

Gửi dữ liệu qua kết nối Internet an toàn

Mọi người thường được khuyến cáo rằng chỉ nên thực hiện việc mua hàng, thanh toán hay chuyển tiền trực tuyến thông qua một đường truyền an toàn, có bảo vệ bằng các giao thức bảo mật mạng tiên tiến. Kẻ xấu thường lợi dụng để có được thông tin cá nhân của bạn bằng cách rình mò ở các mạng Wi-Fi công cộng.

Có lẽ việc mạo hiểm đăng nhập vào tài khoản Facebook hoặc Twitter là một ví dụ thực tế và dễ hiểu hơn nhiều. Nếu bất cứ ai giành được quyền truy cập vào hồ sơ mạng xã hội của bạn, điều đó có nghĩa là bạn đã bị mất mát về thông tin cá nhân, thông tin tài chính thậm chí uy tín cá nhân của mình. Trong thời gian qua, đã có trường hợp nhiều tài khoản Facebook bị kẻ xấu đánh cắp nhằm nhắn tin lừa người thân bạn bè trong danh bạ để nạp tiền điện thoại cho chúng.

Không chỉ vậy, hãy thử tưởng tượng bạn dùng điện thoại di động của mình đăng nhập vào một kết nối Wi-Fi mở ở quán cafe rồi lướt web, truy cập mạng xã hội hay thậm chí mua sắm trực tuyến. Điều đó đồng nghĩa với việc bạn đang tự nguyện chuyển giao toàn bộ thông tin cá nhân của mình qua mạng Internet, vốn là nơi tụ họp của tin tặc hoặc các kẻ trộm danh tính. Thực hiện những việc như vậy ở nơi công cộng đúng là một ý tưởng tồi. Thay vào đó, hãy thao tác tương tự trong một mạng Wi-Fi riêng, có thiết lập các chuẩn bảo mật WEP hay WPA thì dữ liệu sẽ được bảo vệ an toàn hơn nhiều.

Sử dụng giao thức web HTTPS trên di động

Có một số tình huống mà bạn buộc phải sử dụng giao diện web di động để mua sắm trực tuyến, có thể vì không tìm thấy ứng dụng tương thích để tải về trên App Store, hoặc không thể chờ đợi cho đến khi về nhà hay đến văn phòng để sử dụng máy tính.

Những lúc như vậy, khi lần đầu tiên mở trang web trong trình duyệt thì bạn luôn luôn phải kiểm tra giao thức kết nối an toàn HTTPS. Điều này sẽ đảm bảo rằng bất kỳ dữ liệu qua lại giữa điện thoại của bạn và máy chủ dịch vụ bán hàng trực tuyến chỉ được chia sẻ giữa hai phía mà không có sự can thiệp của bên thứ ba. Bạn có thể nhận được rất nhiều rủi ro khi gửi thông tin cá nhân trên Internet thông qua giao thức HTTP không an toàn. Hãy kiểm tra chắc chắn biểu tượng ổ khóa xuất hiện trong địa chỉ trang web bán hàng trước khi thả các mục vào giỏ mua hàng của mình.

HUY THẮNG

Nên thực hiện việc thanh toán trực tuyến thông qua các kết nối an toàn.