

CÁC BIỆN PHÁP AN TOÀN KHI XỬ LÝ GIAO DỊCH TRÊN WEB

Tài kh

Tài khoản (account) “chùa”, hoặc bị đánh cắp từ chủ thẻ đang được bày bán tràn lan trên mạng Internet, thậm chí tại một số diễn đàn tin tức, nó còn được “biếu không”. Đây là một trở ngại rất lớn đối với thương mại điện tử (TMĐT), nhất là tại Việt Nam khi mà TMĐT mới đang trong giai đoạn “sơ khai” nhưng đã bị “vùi dập” tàn nhẫn bởi nạn thẻ giả.

Chỉ tính riêng trang web bán hàng trực tuyến VDC o-nline của Công ty Điện toán và Truyền số liệu (VDC), trong năm 2006 đã phát hiện hàng trăm vụ sử dụng thẻ giả để thanh toán hàng. Đó là chưa kể tới hàng loạt các trang bán hàng trực tuyến khác, chắc chắn cũng phải “sống chung” với nạn thẻ giả.

Dưới đây là một số phương pháp mà các nhà cung cấp dịch vụ bán hàng trực tuyến trên thế giới thường hay áp dụng để xác minh tính xác thực của thẻ thanh toán khi tiến hành giao dịch qua mạng...

1. “Định vị” địa chỉ IP

Trong thế giới TMĐT, biết được thông tin địa lý của người mua có thể giúp ngăn chặn các hành vi gian dối. Công nghệ xác định vị trí địa lý hiện nay có thể cung cấp các thông tin địa lý chính xác từ địa chỉ IP máy tính mà người dùng sử dụng để đặt mua hàng, để từ đó có thể phân loại các khu vực được liệt vào “danh sách đen”. Xác định vị trí bằng địa chỉ IP cũng có thể xác định được vị trí chính xác của người dùng hoặc tính toán được khoảng cách giữa địa chỉ đặt hàng của người mua trực tuyến với vị trí thực của người thực hiện giao dịch. Kết quả thu được sẽ giúp người bán hàng có thể áp dụng thêm các biện pháp định danh (bảo mật) mạnh hơn hoặc khoá tài khoản những khách hàng khả nghi.

2. So sánh địa chỉ IP quốc gia với địa chỉ giao hàng trong hoá đơn

Địa chỉ IP là số nhận dạng mạng duy nhất do ISP cấp cho người dùng mỗi lần truy nhập vào mạng Internet. Vậy nên bạn cần chắc rằng địa chỉ IP quốc gia và địa chỉ thanh toán của hoá đơn phải trùng nhau. Sử dụng các dịch vụ phát hiện gian dối web như FraudLabs có thể giúp bạn phát hiện địa chỉ IP quốc gia của khách đặt mua hàng. Nếu địa chỉ giao hàng và địa chỉ trong hoá đơn của khách hàng là ở Mỹ, nhưng người đặt đơn hàng lại có địa chỉ IP ở Nga, thì chắc chắn đây là một trường hợp gian dối điển hình. Thường nếu người đặt hàng không ở nước ngoài thì người bán

nên gọi điện để xác nhận lại thông tin người sử dụng thẻ tín dụng cho chính xác.

3. Kiểm tra bản “danh sách đen”

Bạn luôn luôn phải chú ý tới các đơn hàng được giao tới địa chỉ ở nước ngoài. Bạn càng phải thận trọng hơn nếu địa chỉ giao hàng nằm ở những nước có “truyền thống” về gian lận điện tử. Theo điều tra của ClearCommerce, danh sách 12 nước đứng đầu bản danh sách đen về gian lận trực tuyến là: Ucraina, Indonesia, Yugoslavia, Lithuania, Ai Cập, Romani, Bungary, Thổ Nhĩ Kỳ, Nga, Pakistan, Malaysia, và Israel. Còn 12 khu vực có tỉ lệ gian lận trực tuyến thấp nhất là: Austria, New Zealand, Đài Loan, Ai-Len, Tây Ban Nhan, Nhật Bản, Switzerland, Nam Mỹ, Hồng Kông, Anh, Pháp và Australia.

4. Địa chỉ e-mail ẩn danh hoặc miễn phí

Hãy chú ý rằng nếu người mua hàng trực tuyến sử dụng các địa chỉ e-mail ẩn danh miễn phí như hotmail.com hoặc yahoo.com thì việc truy tìm tung tích là hầu như không thể. Phần lớn các trường hợp gian lận điện tử sử dụng dịch vụ email miễn phí hơn là các e-mail trả phí. Về lý thuyết, bất cứ ai sử dụng địa chỉ email (dựa trên nền tảng web) hoặc địa chỉ được chuyển tiếp tới (forward) đều truy được địa chỉ của ISP đó.

Trong khi có nhiều khách hàng hợp pháp sử dụng địa chỉ e-mail miễn phí bởi tính tiện lợi và kinh tế, thì hầu hết đối tượng gian lận đều sử dụng địa chỉ e-mail miễn phí để ẩn danh. Tuy nhiên, hầu hết các doanh nghiệp khi đặt mua sản phẩm đều có tên miền riêng và trong trường hợp không có thì họ cũng không sử dụng địa chỉ e-mail miễn phí. Đối với những lý do này, bạn cần có phương pháp thu thập thêm thông tin khi địa chỉ e-mail miễn phí được sử dụng, chẳng hạn như khả năng xác định vị trí địa lý của khách hàng. Bạn cũng cần chú ý tới các tên miền mới đăng ký, bởi những kẻ gian lận có thể dễ dàng đăng ký một tên miền mới bằng thẻ tín dụng đánh cắp để lập nên một chủ thể kinh doanh mới.

5. Kiểm tra máy chủ proxy ẩn danh

Bạn cần kiểm tra xem người đặt mua hàng có sử dụng máy chủ proxy ẩn danh hay không, bởi dạng máy chủ này cho phép người dùng Internet có thể che giấu địa chỉ IP thực. Mục đích chính của việc sử dụng máy chủ proxy là để ẩn mình, tránh bị phát hiện. Trong khi các doanh nghiệp có tên tuổi sử dụng phương pháp này để bảo vệ mạng nội bộ thì những kẻ gian lận lại sử dụng máy chủ proxy cho mục đích che giấu tung tích.

6. Kiểm tra địa chỉ giao hàng

Đương nhiên những kẻ gian lận thường tránh bị phát hiện nhưng điều cốt lõi là cần nhận được hàng. Có một cách để làm được điều này là sử dụng hộp thư công cộng, hoặc sử dụng địa chỉ giao nhận chuyển tiếp. Hãy nhớ là không bao giờ gửi hàng tới hộp thư thuê công cộng (ngoại trừ bạn có thể xác định được hộp thư đó thuộc về khách hàng quen biết) hoặc những địa chỉ giao hàng chuyển tiếp bởi khi đó bạn không thể xác định được địa chỉ thực và danh tính người nhận

hàng.

7. Số điện thoại chính xác, mã ZIP hợp lệ

Thường thì bên giao hàng sẽ phát hiện được các đơn hàng có số ZIP không hợp lệ, hoặc sự không trùng khớp giữa mã ZIP và mã khu vực. Những trường hợp này hiển nhiên tiềm ẩn nguy cơ gian lận nhiều hơn. Ngoài ra, nếu điện thoại sử dụng để liên lạc ở đây là dạng VOIP (như vẫn rất thịnh hành hiện nay) thì việc hoãn lại thời điểm chuyển hàng, nhất là các mặt hàng đắt tiền, sẽ là một quyết định khôn ngoan.

8. Đối chiếu tên quốc gia phát hành thẻ với tên quốc gia trong hoá đơn

Một điểm quan trọng nữa cần ghi nhớ là cần kiểm tra tên quốc gia phát hành thẻ tín dụng và tên quốc gia trong địa chỉ hoá đơn. Tên của chúng cần phải trùng với nhau. Việc này rất quan trọng bởi nhiều ngân hàng nhỏ thường không có các thủ tục xác nhận nghiêm ngặt.

9. Gọi điện cho ngân hàng phát hành thẻ tín dụng

Nếu bên bán cảm thấy nghi ngờ về đơn đặt hàng thì có thể gọi điện cho ngân hàng đã phát hành thẻ tín dụng để phòng trường hợp những chiếc thẻ sử dụng là đồ đánh cắp. Số điện thoại của ngân hàng phát hành thường dựa trên sáu con số đầu tiên của thẻ, thường được biết đến là Số định danh ngân hàng (Bank Identification Number - BIN).

10. Yêu cầu thêm thông tin nếu cảm thấy có vấn đề

Khi giao dịch, chỉ có tên tuổi và số thẻ tín dụng của khách hàng không thôi thì e rằng sẽ không đủ. Bên bán cần cần yêu cầu khách hàng xác nhận qua điện thoại hoặc fax ảnh nhận dạng nếu cảm thấy giao dịch có vấn đề.

Văn Hân