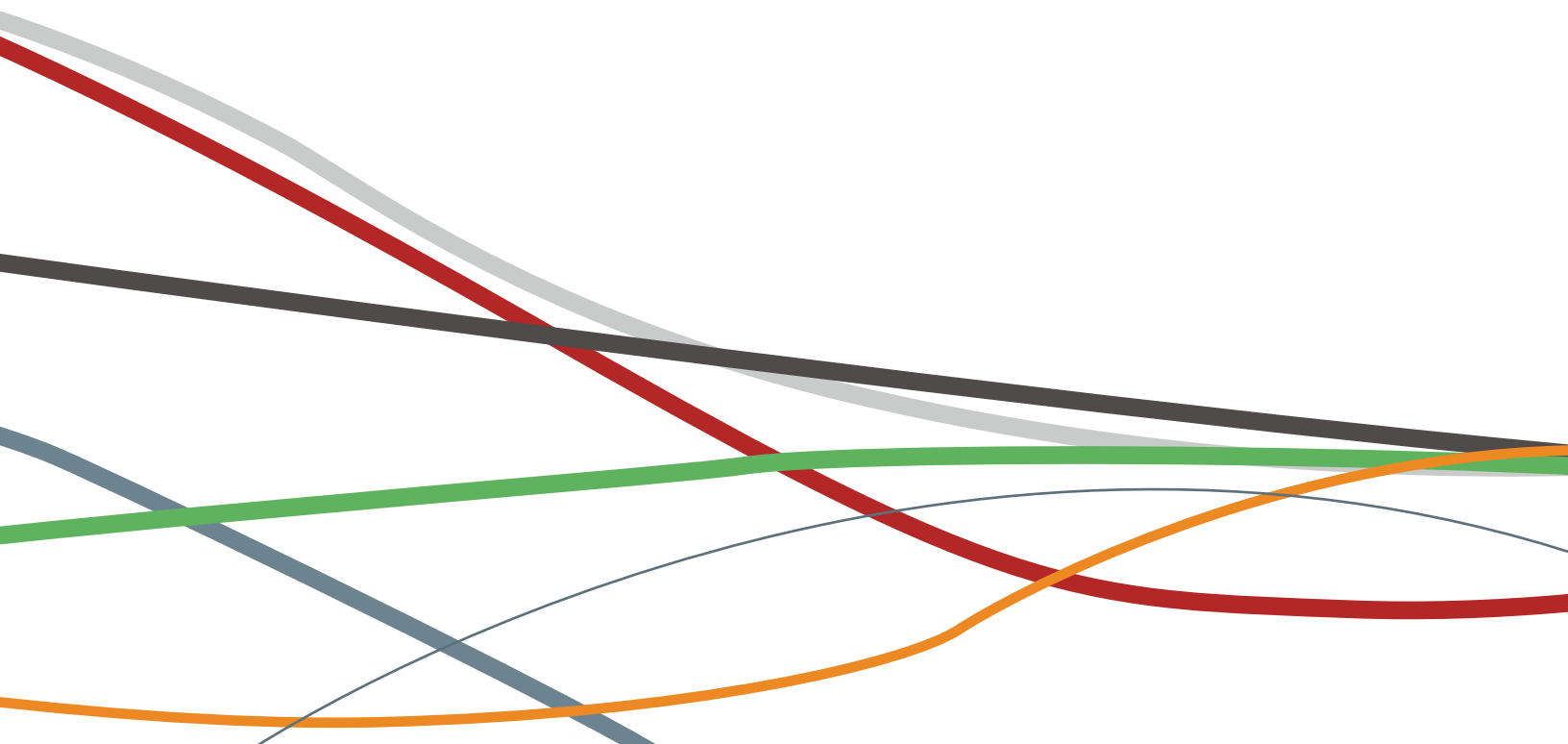


Géolocalisation - Cerner votre ennemi

Novembre 2008
Quova, Marketing Produit

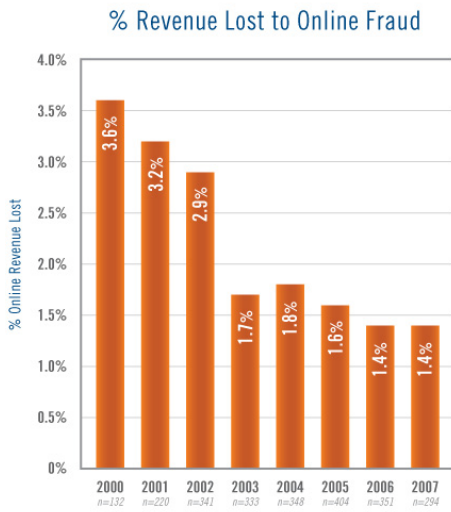


Géolocalisation - Cerner votre ennemi

Sommaire

Cerner votre ennemi	3
Fraude par carte de crédit en ligne: tous les eCommerces sont menacés.....	4
Fonctionnement de la Géolocalisation: Cinq moyens de détecter les fraudes, et exemples réels de la Géolocalisation à l'oeuvre.....	4
Rempporter la lutte.....	8
Au sujet de Quova, Inc.	8

Géolocalisation - Cerner votre ennemi



© CyberSource Corporation, all rights reserved.

Cerner votre ennemi

Avant de commencer toute lutte, vous devez déterminer qui est votre ennemi. En ligne, l'ennemi du marchand est toute personne qui a l'intention de commander des biens ou services avec des numéros de cartes de crédit volées ou de pirater le compte d'un client.

Prenons le cas réel d'un marchand en ligne. En une journée, ce marchand de la côte est des Etats-Unis a reçu des commandes d'une valeur totale de près de 500 000 USD pour des télévisions plasma haut de gamme avec un écran de 42 pouces. Une journée record peut-être? On aurait pu le croire au premier abord. Toutes les commandes avaient été payées avec des cartes de crédit aux numéros différents et les noms et adresses de facturation et d'expédition étaient tous différents également. Tout semblait en ordre. Toutefois, en raison du volume inhabituel, le système de contrôle des risques du marchand a signalé la nécessité de procéder à une revue manuelle des commandes. Chacune de ces commandes apparemment différentes provenait du même fuseau horaire et d'un ordinateur dont le navigateur avait été configuré en langue russe. C'était peut-être une coïncidence, mais c'était plutôt inhabituel. La probabilité que différents clients parlant tous le russe et résidant tous dans le même fuseau horaire veuillent acheter des télévisions plasma avec un écran de 42 pouces était plutôt faible. Et puis il y a eu le moment décisif. Le marchand a vérifié toutes les adresses IP, un numéro unique attribué à un ordinateur ou dispositif particulier pour acheminer les messages. Toutes les commandes provenaient de la même adresse IP, même si les adresses de facturation et de livraison étaient différentes pour chaque commande. Ce n'était en fait pas une journée record, et sans le service de géolocalisation de ce marchand, il aurait expédié des milliers de dollars de télévisions plasma sans grand espoir d'être payé ou de pouvoir récupérer la marchandise.

Le fait de savoir où se trouvent les personnes qui consultent votre site Internet est de plus en plus important pour les entreprises en ligne, afin de leur permettre de prendre des décisions commerciales en temps réel pour éviter les fraudes, de respecter les réglementations, de gérer le contenu numérique, d'exécuter les stratégies de marketing et de se protéger contre les attaques en ligne. Ce rapport fournit un aperçu des mesures prises par les fraudeurs en ligne et qui font tort aux e-marchands et à leurs clients. Il indique également la façon dont la géolocalisation s'est établie comme l'un des outils les plus efficaces pour identifier les activités frauduleuses en ligne.

Divulgations: Ce rapport, parrainé par le prestataire de géolocalisation IP, Quova, Inc., illustre la façon dont les sociétés utilisent la géolocalisation pour les aider à détecter les fraudes au niveau des transactions par carte de crédit en l'absence du titulaire de la carte, et il contient des informations recueillies auprès d'experts de l'industrie et de clients de Quova. Tous les tableaux proviennent de l'édition 2008 du « Online Fraud Report » produit par CyberSource Corporation, un partenaire de solution de Quova.

Géolocalisation - Cerner votre ennemi

Fraude par carte de crédit en ligne: tous les e-marchands sont menacés

Nous connaissons désormais le résultat de la neuvième édition annuelle 2008 du "Online Fraud Report" de Cybersource, un grand prestataire de solutions de gestion des paiements électroniques, des risques et de la sécurité. Sur 318 vendeurs interrogés en ligne, des nouveaux e-commerces de petite taille aux plus grands e-détaillants et organismes de distribution numérique à travers le monde, le rapport indique qu'en moyenne 1,4 % des commandes sont perdues en raison de fraudes en ligne. La fraude résulte le plus souvent des acheteurs qui utilisent des numéros de carte de crédit ultérieurement identifiés au titre de cartes volées. Votre entreprise ne sera vraisemblablement pas différente.

"Nous estimons qu'en 2007, 3,6 milliards de dollars de revenus en ligne ont été perdus à cause d'activités frauduleuses" explique Doug Schwegman, directeur de la clientèle et de l'intelligence commerciale de CyberSource Corporation. "Et cela ne représente qu'une partie du problème. La même année, les marchands américains et canadiens ont refusé en moyenne 4,2 % de leurs commandes pour présomption de fraude. Vous pouvez être sûr qu'il y a des commandes valides dans ce groupe de commandes refusées, ce qui représente un montant de pertes supplémentaires important. Pour les commandes qui proviennent de pays autres que les Etats-Unis et le Canada, le pourcentage de commandes refusées pour présomption de fraude était 2,5 fois plus élevé."

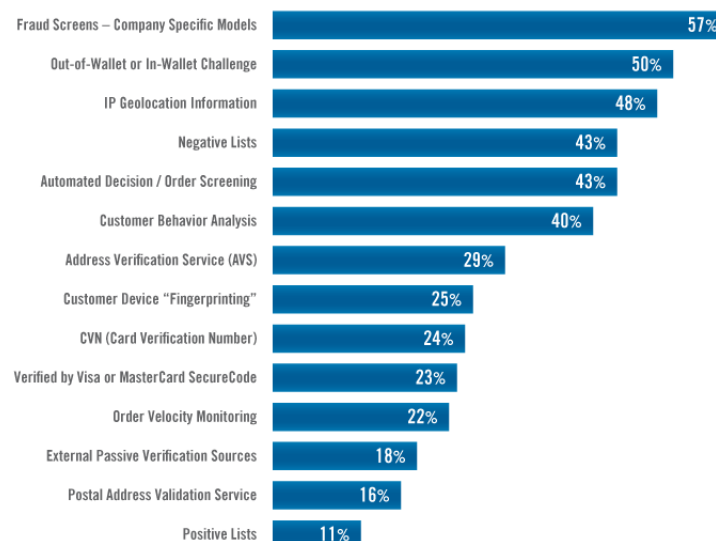
De nombreuses transactions frauduleuses sont détectées de nos jours, grâce à une grande diversité d'outils de détection. "Le message le plus important que nous communiquons à nos marchands est qu'il n'existe pas d'outil miracle" explique Schwegman. "Les marchands doivent employer tout un arsenal d'outils. L'époque des adolescents fraudeurs est bel et bien révolue. Les coupables font désormais ce travail à temps plein et utilisent des méthodes sophistiquées. Nous devons être plus sophistiqués qu'eux pour les vaincre."

Même si la géolocalisation est juste l'un des outils de contrôle des risques qui sont utilisés (le marchand en ligne moyen utilise au moins quatre outils), elle fournit une ligne de défense robuste. La localisation géographique d'une transaction proposée peut être un indicateur important de fraude potentielle, particulièrement lorsque la localisation ne correspond pas à l'adresse physique fournie par le client. Dans le monde réel, une demande de carte de crédit bancaire comportant le cachet postal de l'Ukraine susciterait indubitablement certaines inquiétudes dans le bureau de crédit. Une tentative d'achat en ligne présentant une contradiction similaire susciterait une alarme du même type: les recherches menées par Experian sur les tendances en matière d'identité frauduleuse ont déterminé que lorsqu'un client s'inscrit en fournissant une adresse dans un état américain particulier mais qu'il passe la commande dans un autre état, ceci peut être un indicateur prédictif de fraude. Les transactions effectuées à travers les frontières nationales suscitent encore davantage d'inquiétudes. Les transactions internationales représentent près de la moitié de toutes les récupérations sur carte de crédit, et une courte liste de pays (Ghana, Vietnam et Liban entre autres) sont responsables des transactions les plus frauduleuses.

"Dans le monde de la prévention des fraudes, nous avons vraiment besoin de savoir où vous êtes" explique le responsable du projet fraude d'un grand portail Internet et site de moteurs de recherche, un usager à long terme du service de géolocalisation de Quova. "C'est outil a été d'importance critique."

En connaissant le niveau de risque, les marchands peuvent utiliser la géolocalisation pour indiquer les transactions douteuses et les aborder de manière individuelle. Lorsque le risque dans un endroit particulier est extrême, cet endroit peut être totalement bloqué. C'est là une étape que la plupart des entreprises hésitent à prendre en raison du risque de blocage des clients légitimes, ce que l'on appelle souvent des "faux positifs." Cependant, à la lumière des pertes bien connues subies par certains prestataires financiers en ligne, les efforts effectués pour adresser les risques de fraude servent non seulement à protéger les résultats de l'entreprise mais également à convaincre les consommateurs que le marchand fait tout ce qui est en son pouvoir pour empêcher que les fraudeurs ne puissent utiliser les cartes de crédit volées.

Most Effective Fraud Management Tools
% of Merchants who selected tool as one of their three most effective*



Géolocalisation - Cerner votre ennemi

Fonctionnement de la géolocalisation: Cinq moyens de détecter les fraudes et exemples réels de la géolocalisation à l'oeuvre

Aucun des outils de protection contre les fraudes en ligne n'est à l'abri de toutes les menaces. Toutefois, chacun d'entre eux ajoute une couche de protection supplémentaire pour les marchands qui doivent faire face à des fraudes potentielles, et chacun est renforcé du fait de connaître quelques pratiques des marchands.

"On pense à tort que si vous savez où se trouve une adresse IP, vous savez où se trouve l'utilisateur" explique Kevin Ryan, directeur des solutions clients de Quova, Inc., qui utilise les adresses IP dans le cadre de son processus de géolocalisation. "Mais la localisation des usagers peut en fait varier considérablement."

Il y a de nombreuses façons pour les acheteurs de se connecter à un site Internet d'e-commerce, des points d'accès WiFi publics aux ordinateurs à domicile en passant par les ordinateurs portables quand ils sont en déplacement. Chaque moyen d'accès présente son propre jeu de défis quant à savoir exactement d'où vient l'acheteur. En matière de géolocalisation, les marchands dont les taux de détection de fraude sont les plus élevés commencent par cinq secteurs clés où il est vraisemblable de détecter des commandes frauduleuses.

Vérifier les serveurs de proxys anonymes et les autres systèmes qui dissimulent la localisation: Les serveurs proxy acheminent les communications entre votre ordinateur et l'Internet. Même si tous les serveurs proxy ne sont pas de mauvais augure, l'usage d'un serveur proxy anonyme qui cache ou masque votre adresse IP unique peut être un indicateur de fraude. Pour utiliser un proxy anonyme, un visiteur Internet doit au préalable se connecter à un serveur ou à un site Internet comme Anonymizer.com (les usagers

paient entre \$19,99 et \$ 99,99 par mois) ou à des services gratuits compatibles aux achats, comme Proxify.com ou The-Cloak.com, avant de pouvoir consulter l'Internet. Ces systèmes déguisent l'adresse IP en lui substituant l'IP de la localisation de l'anonymiseur.

Souvent, cette démarche est effectuée de manière légitime, par des citoyens soucieux de garder leur anonymat ou qui souhaitent éviter les cookies et les scripts quand ils sont sur l'Internet. Ces clients ne bénéficient pas d'un contenu localisé, de connexions plus faciles et de pages Internet personnalisées, mais pour beaucoup c'est un compromis acceptable. A d'autres moments, cette démarche est effectuée par les acheteurs qui souhaitent contourner leurs connexions au navigateur de leur travail ou de leur domicile, de manière à ce que les commandes qu'ils passent ne soient pas connues de leur société ou des membres de leur famille. De nombreux lycéens et étudiants utilisent de nos jours des proxys anonymes pour éviter les filtres scolaires placés sur Facebook et YouTube. Trop souvent, toutefois, cette démarche est effectuée par des prédateurs et des fraudeurs qui essaient d'éviter la détection. "Il y a maintes façons de pirater votre adresse IP, soit de manière anonyme soit en payant" explique le responsable des fraudes du site de moteurs de recherche. "Ainsi, il vaut la peine de profiter des listes de proxys anonymes d'un prestataire de géolocalisation" explique-t-il.

Les listes de proxys anonymes qui abusent du système, fournies par quelques vendeurs de géolocalisation, informent le marchand de l'arrivée d'une commande par un serveur proxy. Les marchands qui utilisent le service GeoPoint Gold Edition de Quova, par exemple, peuvent programmer leur logiciel d'achat pour décliner ou faire la revue des commandes envoyées par des proxys anonymes.

Entre temps, la localisation de certains acheteurs est peut-être masquée sans qu'ils ne l'aient souhaité. Les commandes

passées par téléphone cellulaire ou dispositif mobile peuvent être difficiles à tracer. "Pour localiser un téléphone cellulaire non-GPS, vous devez pouvoir accéder aux informations de la tour cellulaire" explique Ryan à Quova. Pour combler le vide, plusieurs prestataires de services de géolocalisation comme Quova ont établi un partenariat avec des prestataires GPS virtuels, comme Mexens Technology, dont l'application Navizon fait le suivi du positionnement de la tour cellulaire et de WiFi. "Grâce à Navizon, les marchands peuvent accéder à une grande base de données de plus en plus importante de points d'accès cellulaire et WiFi aux quatre coins du globe" explique Ryan. "Nous pouvons vérifier la localisation d'un combiné en utilisant un petit morceau de code inséré par le fournisseur de combiné ou une application exploitée par-dessus."

C'est quelque chose qui plaît vraiment aux marchands: "Nous avons fait des démonstrations de technologies vraiment fascinantes en utilisant les téléphones cellulaires et en détectant les localisations" explique le responsable de fraude du site de moteurs de recherche. "Quova offre de nombreuses fonctions supplémentaires qui rehaussent vraiment la barre et maintiennent nos concurrents sur le qui-vive."

Les connexions par réseau commuté présentent une autre sorte de défi. Les commandes passées par le biais d'une connexion Internet par réseau commuté sont au préalable acheminées par le serveur sur réseau commuté du prestataire, avant d'arriver sur le site du marchand. Ainsi, un usager d'EarthLink qui se déplace dans Londres mais qui utilise un réseau commuté pour se connecter à son fournisseur d'accès à Internet basé en Californie, donnera l'impression d'être en Californie et non pas à 9600 km de là.

Les clients AOL font également exception car AOL utilise un serveur central. Ainsi, tous les clients d'AOL semblent se connecter à partir de Herndon, en Virginie, où se trouve l'un des principaux

Géolocalisation - Cerner votre ennemi

serveurs d'AOL (même si cette question est devenue pratiquement redondante, car AOL continue de perdre des clients de navigateur AOL). "Pour beaucoup, le réseau commuté est le moyen de communiquer en étant de l'autre côté du monde mais en prétendant être sur place" explique Ryan. Les serveurs sur réseau commuté sont toutefois de plus en plus sophistiqués, et nombre d'entre eux indiquent désormais au minimum des identifiants basés sur l'indicatif régional pour leurs utilisateurs.

Ce type de serveurs, qui masquent la localisation, présente un défi pour les marchands qui utilisent la géolocalisation, mais le problème n'est pas insurmontable. Certains marchands incorporent des règles commerciales dans leur application d'achat pour rejeter les commandes d'acheteurs qui n'utilisent pas une ligne Internet à haute vitesse fixe. Toutefois, cette stratégie élimine également de nombreux acheteurs légitimes. Pour améliorer les taux d'acceptation, d'autres marchands préfèrent être avertis des commandes en provenance de connexions Internet non fixes, comme déterminé par la géolocalisation, pour effectuer une revue manuelle des risques. S'ils détectent un schéma particulier de commandes frauduleuses, c'est seulement alors que certains types de connexions seront autorisés.

Vérifier la distance entre les localisations réelles et attendues de l'utilisateur: En règle générale, les acheteurs se connectent sur Internet depuis un endroit proche de leur adresse de facturation ou d'expédition. La géolocalisation fournit un moyen facile de vérifier la véritable localisation du client. Les marchands qui utilisent la géolocalisation peuvent également faire la revue du code postal et de la latitude et longitude associées à l'adresse IP de l'acheteur. Ces informations peuvent être vérifiées non seulement par rapport aux informations fournies par l'acheteur, comme son adresse de facturation ou

de livraison, mais aussi par rapport aux informations sur l'inscription ou les séances précédentes de cet utilisateur, pour trouver une distance entre la localisation réelle et la localisation attendue de la personne qui passe la commande en ligne. De nombreux clients de Quova signalent que les commandes qui proviennent d'au moins 800 km de la localisation attendue sont plus probablement frauduleuses. Avec la géolocalisation, les marchands peuvent choisir de décliner ou de signaler pour revue les commandes passées à au moins X km de l'adresse d'expédition ou de facturation. Voici comment un client de Quova, un site de réservation touristique en ligne qui effectue près d'un milliard de dollars de ventes par an, y parvient: "Notre système anti-fraude se trouve en dehors de notre itinéraire d'achat" explique le directeur des risques et revenus de l'e-commerce. "Nous captions les adresses IP au moment de l'achat; nous interrogeons la base de données de Quova pour obtenir la géolocalisation de cette adresse IP et nous en tenons compte dans le score de risque. Chaque jour, nous voyons des adresses de facturation de cartes qui ne correspondent pas à la localisation de l'adresse IP; c'est un excellent indicateur de fraude."

Utilisation des informations sur le domaine pour évaluer les risques: La plupart des prestataires de données de géolocalisation fourniront au marchand des informations sur le domaine obtenues à partir de l'ISP de l'acheteur, et utiliseront ces informations supplémentaires pour déterminer si une commande devrait être refusée, acceptée ou signalée. Par exemple une commande passée sur un ordinateur professionnel et transmise par le serveur de la société sera identifiée par l'adresse du site Internet de la société, comme IBM.com. Une commande passée d'un bureau du gouvernement sera identifiée par l'extension .gov ou .mil. Une commande passée par un consommateur à domicile qui utilise un IP comme Comcast ou

British Telecom aura comme adresse de domaine @comcast ou @BT. Un marchand peut également faire le suivi des séances de l'utilisateur et savoir que le client se connecte souvent de son travail et de son domicile. "Pour le trafic des consommateurs et des petites entreprises ainsi que pour les connexions de recherche à domicile, vous ne verrez généralement que les informations du prestataire d'e-mail, comme johnsmith@cox.net. Pour les plus grandes entreprises, en plus du nom de domaine de la société, vous verrez entre autres les informations de la société dans le nom de domaine de l'e-mail, comme IBM.com et dans les données de connexion de géolocalisation fournies vous verrez probablement une connexion à vitesse plus rapide, comme une connexion OCX ou T1 ou supérieure" explique Ryan. "Les domaines professionnels peuvent également confirmer la légitimité d'une demande d'expédition à une adresse professionnelle."

Même si certains domaines peuvent être utilisés pour confirmer l'identité d'un acheteur, d'autres domaines peuvent susciter une alarme. Ainsi, on trace souvent les origines des fraudes au niveau de serveurs universitaires, où quiconque s'est jamais inscrit à un cours, même un étudiant par correspondance ou un ancien étudiant, peut obtenir une adresse .edu gratuite aux Etats-Unis ou une adresse ac.com gratuite au Royaume-Uni. Des taux de fraude élevés ont également été détectés dans les serveurs de centres de copie qui louent des périodes d'ordinateur, comme Kinkos.com. "Il existe des risques potentiels associés à certains d'entre eux" explique Ryan. "Selon vos activités et le type de produit que vous vendez, certains domaines sont un peu plus menacés que d'autres. Par exemple, les centres de copie qui louent des périodes de serveur, comme Kinkos.com, peuvent être une source d'inquiétude pour un marchand qui vend des articles onéreux, comme du matériel informatique d'entreprise, mais pas pour un marchand qui vend des articles de

Géolocalisation - Cerner votre ennemi

consommation à bas prix, comme les CD et les livres. Un consommateur qui utilise un ordinateur loué pour passer une commande pour un CD ne pose pas de problème, mais pourquoi utiliser un ordinateur loué pour passer une commande de matériel informatique d'entreprise?" Avec la géolocalisation, le marchand peut prendre ces informations et programmer le caddie pour décliner ou signaler les commandes avec les extensions de domaines .edu, "copycenter".com ou autres extensions de domaines problématiques.

Construire des profils d'utilisateur:

La géolocalisation fournit un moyen facile pour les marchands d'élargir leurs profils d'utilisateurs en coulisses. "Nous les utilisons pour comparer d'où vient ce consommateur par rapport aux données du client qui ont été saisies, par exemple l'adresse de facturation et l'adresse d'expédition" explique le directeur des risques du site touristique. "Il nous fournit davantage de données sur les consommateurs pour vérifier qui est vraiment le client.

"Les données de géolocalisation peuvent être enregistrées aux côtés des informations fournies par les acheteurs au moment de leur inscription. Les inscriptions du client peuvent être associées aux extensions de domaine fournies, aux adresses IP, aux informations de latitude et de longitude, aux codes postaux et même à la quantité de temps qu'un utilisateur connu passe sur le site Internet d'un marchand dans le cadre du traitement de la commande. A chaque fois que quelqu'un utilise le compte de cet acheteur, le service de géolocalisation permet de vérifier si la connexion provient du même endroit que celui où se trouvait l'acheteur légitime au moment de son inscription. Bien sûr, le profil de

géolocalisation peut changer selon l'usage de café Internet ou les déplacements, mais le système suppose que la plupart des commandes valides adoptent le même schéma. Si des extensions de domaine ou des IPS différents sont utilisés le même jour, il y a des chances pour que ces commandes soient frauduleuses.

Lorsqu'un profil a été construit, les marchands peuvent chercher les changements, les différences entre les comportements observés qu'ils voient en ligne et ceux qu'ils ont dans leurs fichiers. "Ainsi, si l'utilisateur vient toujours du même ISP mais que sa localisation a soudainement changé de 80 km, ceci pourrait être inquiétant" explique Ryan. "Et dans le cadre des acheminements ou enroutements fixes, si une personne se trouve en dehors d'un rayon de 80 km, ce que l'on considère généralement être la plus grande zone métropolitaine, ceci pourrait indiquer que l'utilisateur a physiquement changé de domicile ou de travail, ou qu'il s'est fait voler sa carte de crédit ou encore que son compte client a été piraté."

Certains marchands abordent ce problème en créant des profils d'utilisateur pour la maison, le travail et les déplacements, de manière à ce que les commandes valides soient automatiquement comparées avec ces profils valides. Ceci permet d'éviter nombre de refus accidentels possibles. Si un utilisateur a déménagé, il est bon que le marchand établisse le contact avec l'utilisateur pour lui demander et vérifier sa nouvelle adresse ou qu'il conserve la commande jusqu'à ce que la nouvelle adresse soit vérifiée.

Utiliser les informations sur le fuseau horaire pour faire le suivi de la "vélocité" de la transaction: "Si un utilisateur effectue des connexions à un site Internet durant des périodes de temps relativement courtes et si les connexions sont à plus de 1600 km de distance les unes des autres, voilà un signal d'alarme" explique Ryan. "Même si ça pouvait être quelqu'un en déplacement ou qui partage un compte avec son épouse ou ses enfants, il est également tout à fait possible que quelqu'un ait compromis ce compte."

Pour chaque acheteur, les marchands peuvent utiliser les données de géolocalisation afin d'activer des règles commerciales qui 1) exigent l'heure locale actuelle à la localisation de l'acheteur; 2) les alertent des "sauts de fuseaux horaires" potentiels en une courte période de temps, en cas d'accès au même compte depuis plusieurs localisations géographiques; et 3) leur signalent les commandes passées à des heures de la journée qui sont irrégulières par rapport aux commandes précédentes enregistrées dans le profil de l'utilisateur.

Certains marchands prennent tous ces scénarios et créent des systèmes logiciels qui utilisent les données de géolocalisation pour détecter encore d'autres risques de fraude. Prenez un client de Quova, une société financière américaine qui offre des applications en ligne pour les cartes de crédit de marque privée, les prêts personnels, les cartes bancaires et les assurances crédit. "La façon dont nous avons utilisé les données de géolocalisation de Quova est très avancée; et elle doit l'être" explique son directeur de stratégie de lutte contre la fraude. "Elle nous donne un réel avantage sur la concurrence dans notre travail Internet.

Géolocalisation - Cerner votre ennemi

Remporter la lutte

Il n'est pas rare qu'un site Internet fasse le suivi du comportement des usagers, comme les pages sur lesquelles ils cliquent et les produits qu'ils achètent. C'est ce qu'on appelle le ciblage de comportement et certains experts sur la vie privée s'inquiètent que ceci va un peu trop loin. Avec la géolocalisation, on n'accède jamais à l'ordinateur du client. La géolocalisation est une question de sécurité, pour protéger le consommateur et le marchand contre les activités frauduleuses. Grâce à la géolocalisation, souvent le marchand sait généralement où notifier la mise en vigueur de la loi locale pour attraper le coupable en flagrant délit.

En fin de compte, la géolocalisation est "seulement l'un des nombreux moyens que vous pouvez utiliser pour vérifier le cycle de fraude. C'est juste l'un des outils à votre disposition" explique le responsable des fraudes du site de moteurs de recherche. "Mais nous l'utilisons et nous étudions les cas de fraude qui passe à travers le filet en faisant la revue des récupérations [les commandes par carte de crédit qui sont contestées]. Notre taux de fraude est plutôt faible, nous sommes à moins de 0,5 %, pour la société entière."



Au sujet de Quova, Inc.

Quova Inc. est le premier prestataire de données de géolocalisation sur Internet. Il a pour objectif de donner aux entreprises en ligne la possibilité de déterminer immédiatement où se trouvent leurs visiteurs Internet sur le plan géographique. Les données de Quova touchent des milliards de visiteurs Internet chaque jour et sont utilisées par les entreprises en ligne pour géocibler leur publicité et leur contenu, détecter le vol d'identité et les fraudes en l'absence du détenteur de la carte de crédit, gérer la distribution des téléchargements numériques, optimiser le facteur analytique de l'Internet et veiller au respect des réglementations. La plate-forme Location Intelligence brevetée de Quova va au-delà des technologies traditionnelles de géolocalisation IP et de l'intelligence IP et elle fournit des données démographiques détaillées et des données sur les caractéristiques du réseau, allant dans certains cas jusqu'au quartier d'une ville particulière. Les données sont exactes à 99,9 % au niveau du pays et 96 % au niveau de l'état américain (recherches indépendantes menées par Pricewaterhouse Coopers). Quova détecte également l'utilisation des serveurs proxy, qui indique souvent une fraude potentielle, et contrôle pratiquement un demi-milliard de proxies anonymes dans le cadre de ses optimisations de données hebdomadaires. La base de clients de Quova réunit les 3 principaux moteurs de recherche du monde et des milliers de vendeurs sur Internet, agences interactives, réseaux publicitaires, diffuseurs, banques, opérateurs de jeux et agences gouvernementales. Pour tous renseignements complémentaires, veuillez consulter le site www.quova.com

Quova, Inc. est une société privée qui compte parmi ses investisseurs Mobius Venture Partners et IDG. La société Quova a été fondée en 2008. Elle est basée à Mountain View, en Californie.

Copyright © 2010 Quova, Inc. Tous droits réservés. Quova, le logo de Quova et GeoPoint sont des marques commerciales, des marques déposées ou marques de services de Quova, Inc. aux Etats-Unis et dans certaines autres juridictions du monde. Tous les autres noms de sociétés et de produits peuvent être des marques commerciales, marques déposées ou marques de service de leurs propriétaires respectifs.