

Diseño para prevenir el fraude

Juan Leal . Madrid, España.

Introducción

El término fraude, en su sentido más amplio, hace referencia a un engaño con el objetivo de obtener ganancias personales. Esta acción es un crimen y, como tal, está perseguida por la ley. Las estafas económicas son quizá el tipo de fraude más común, pero también se da en otros entornos, como el arte, la arqueología o la ciencia¹.

Combatir el fraude es un trabajo delicado y meticuloso al que es necesario dedicarle importantes recursos. En el mundo online, el diseño de interacción debe ocupar un lugar destacado en esta lucha.

Diseñar para lo más probable y no para todo lo posible², un axioma ampliamente extendido en el diseño de interacción, puede llegar a ser un arma de doble filo en la lucha contra el fraude: “Lo más probable” es que la mayoría de los usuarios empleen la web según los objetivos inicialmente definidos para el negocio online. Pero cuando se habla de fraude por Internet, es necesario tener en cuenta también ese porcentaje de “todo lo posible”.

Conocer qué parámetros son utilizados para realizar acciones fraudulentas disminuye costes y preocupaciones, aumentando al mismo tiempo la fidelización de usuarios, su nivel de satisfacción y mejorando la experiencia de uso en la web.

¹ Fraud definition. <http://en.wikipedia.org/wiki/Fraud>.

² The Inmates Are Running the Asylum. 2000. Alan Cooper.

Este artículo se centra en dos escenarios que frecuentemente permiten el uso fraudulento de información:

- La obtención del e-mail como dato para realizar acciones fraudulentas (suplantación de personalidad, spam y otras).
- La fiabilidad de los sistemas de reputación como elemento para combatir la estafa.

Cómo diseñar para combatir el fraude

En Internet, el fraude ocurre principalmente en aquellas webs conocidas como transaccionales. Alan Cooper denomina webs transaccionales a aquellas que van más allá del click and search, ofreciendo funcionalidades que permiten a los usuarios conseguir algo más que información³. Ejemplos de webs transaccionales son las webs de subastas, de viajes o de servicios financieros.

Algunos de los fraudes más conocidos en las webs transaccionales son:

- Operaciones a través de tarjetas (o datos de tarjeta) de crédito robadas;
- Compra-venta de artículos;
- Envíos de dinero (en sus versiones Nigeriana, Europea y China);
- Oportunidad de negocio / trabajo desde casa;
- Fraude por click;
- Phishing;
- Pharming.

El uso fraudulento de una web normalmente es protagonizado por usuarios expertos, aquellos que mejor la conocen. Cuando se lanza un negocio online, es necesario tiempo para detectar casos de uso anómalos. Al tener poco tráfico y un escaso número de usuarios, este tipo de tendencias no resulta fácil de detectar.

Con un nivel de tráfico regular y constante y un volumen de páginas importante, en algunas secciones de la web pueden asomar ciertas debilidades que usuarios

con malas intenciones podrían utilizar en su propio beneficio, bien para sacar provecho personal de la web o bien para sacar provecho de los usuarios que la utilizan. Pensar en un diseño de interacción que no de pie al fraude empieza a ser necesario.

Uno de los aspectos más importantes es tener claro qué parámetros pueden servir para detectar el fraude. Un primer paso es conocer el alcance de lo que se puede hacer con la base de datos. Cuanto más reciente sea la base, mayor flexibilidad tendrá, aumentando las posibilidades de cruzar más parámetros que facilitarán la detección de un uso anormal.

Dependiendo del negocio al que esté enfocado la web, algunos parámetros servirán más que otros. Ejemplos de parámetros que podrían servir para realizar acciones fraudulentas son los siguientes:

Parámetros internos (menor probabilidad de ser visualizados en la interfaz):

- Movimiento en las fechas de alta y baja;
- Cambios realizados sobre un producto (precio, características...);
- Cambios de dirección de email o nick de usuario;
- Datos personales de otra índole: telefónicos, dirección física.

Parámetros externos (se visualizan en la interfaz):

- Comentarios o reseñas que los usuarios realizan al final de una transacción;
- Red social de un usuario;
- Escalas de satisfacción;
- Calidad de las respuestas en relación a un producto.

Tras la elección del parámetro llega el trabajo de diseño, tanto de información como de interacción. Dos interrogantes claves aparecen en este escenario: qué información mostrar y cómo mostrarla.

³ About Face 3. The Essentials of Interaction Design. 2007. Alan Cooper, Robert Reimann y David Cronin.

1. Qué información mostrar

Conocer hasta dónde se puede llegar con la información que se muestra en la interfaz es un trabajo fino y delicado.

Paradójicamente, ser demasiado transparente a la hora de informar a los usuarios -premisa fundamental en diseño de interacción- puede tener efectos adversos sobre el negocio, ya que la información mostrada puede ofrecer valiosas pistas y ser empleada para explorar nuevas oportunidades de fraude.

Un pequeño ejemplo:

Supongamos que un usuario, para registrarse en una determinada web, necesita introducir su e-mail y su número de teléfono. Al confirmar sus datos, el sistema detecta que ya existe otro usuario con el mismo número de teléfono y le muestra un mensaje de error. Las alternativas para la redacción del contenido de este mensaje nos enfrentan ante el paradigma de Cooper, “Lo probable frente a lo posible”:

- a) Lo más probable: El usuario que se está registrando ha estado anteriormente registrado con otra dirección de e-mail y el mismo número de teléfono. Lo más probable es que no recuerde con qué cuenta de correo se registró. Con informarle en el mensaje de error de cuál era su antiguo e-mail sería más que suficiente;
- b) Lo posible: existe también la posibilidad de que el

usuario que se está registrando pretenda hacer un uso fraudulento de determinadas cuentas de correo y esté tratando de adquirirlas a través de las debilidades que ofrece la interfaz. Mostrando la dirección de correo en el mensaje de error se facilitaría aún más dicha labor.

Una solución para evitar el fraude es mostrar sólo una parte de la dirección de correo, como se muestra en la figura 1.

Con esta solución se evita por un lado el fraude, no mostrando completamente la dirección de correo electrónico, y por otro se ofrecen a los usuarios “perdidos” pistas que pueden ayudarle en la recuperación del error.

2. Cómo mostrar la información

La elección del parámetro que actuará como filtro para detectar el fraude es un condicionante a la hora de definir cómo se va a mostrar la información en la interfaz.

Si se emplean parámetros internos (direcciones de email, teléfono, fechas de alta o baja, etc.) el diseño irá más encaminado hacia el desarrollo de páginas y mensajes muy concretos que aparecerán en determinadas acciones de usuarios, bajo un flujo de navegación muy específico, como se muestra en el ejemplo tomado de Idealista en la Figura 1.

anuncios con el mismo teléfono pero distinto email (distinto usuario)

según nuestros datos estos anuncios han sido introducidos por un usuario con otro email pero tu mismo teléfono

casa o chalet independiente en venta 300.000 € en badajoz, código idealista vw566125
anuncio puesto por juan, con el email juan.leal@---.---
<http://www.idealista.com/pagina/inmueble?codigoinmueble=vw566125>

:: Figura 1: idealista.com informa al usuario de lo que sucede, pero no muestra toda la información existente para evitar el uso fraudulento de la dirección de correo electrónico.

En ese sentido será necesario, aparte de un buen diseño, una sólida arquitectura de información para conocer el flujo de pantallas adecuado y, sobre todo, diseñar pensando en las páginas de error⁴. Este punto adquiere especial relevancia, ya que cualquier usuario se puede encontrar con este tipo de páginas accidentalmente y llegados a este punto, no saber qué hacer al llegar a ellas. Son los denominados Crisis Points⁵, o pantallas que la gente ve cuando algo va mal (Defensive Design for the Web, 2004).

En cualquier caso, resulta muy importante ofrecer siempre claras alternativas de salida en este tipo de páginas y, sobre todo, ser humilde, asumiendo el error como propio y ofreciendo un contacto alternativo, ya que en determinadas ocasiones el error puede ser interno, del sistema.

Si se emplean parámetros externos (escalas, comentarios de otros usuarios, reseñas, red social del usuario, etc.) el enfoque a nivel de diseño de interfaz irá más encaminado hacia módulos con información permanente y actualizada de estos parámetros en determinadas secciones de la web.

Estos módulos tienen una función simplemente preventiva, ya que la decisión final será del usuario que, en función de la información mostrada, actuará de una forma u otra, pero siempre de manera voluntaria. El problema de estos módulos es que no evitan el fraude, tan sólo tratan de minimizarlo.

Un ejemplo de este tipo de módulos lo tiene eBay, portal donde millones de usuarios desconocidos realizan transacciones diariamente.

El sistema de reputación de eBay, basado en el feedback que los usuarios ofrecen al final de una transacción, constituye una potente herramienta en la que apoyarse antes de realizar cualquier operación de

⁴ Diseño de procesos. Jesús Encinar. http://www.jesusencinar.com/2006/08/diseo_de_proces.html

⁵ Defensive Design for the Web. How to improve Error Messages, Help, Forms, and Other Crisis Points. 2004. Matthew Linderman y Jason Fried.





:: Figura 2: Sistema de reputación de un usuario basado en el feedback proporcionado por otros usuarios tras realizar un proceso de compra-venta.

compra-venta. La reputación de los usuarios resulta clave para tener éxito en cualquier proceso transaccional y ayuda a mantener tasas de satisfacción de usuarios muy elevadas⁶.

A pesar de todo, este sistema presenta ciertas debilidades, ya que la tasa de votos positivos podría ser alterada.

Otro ejemplo de este tipo de módulos se puede encontrar en Amazon, portal de compra online, donde las reseñas bibliográficas que los lectores hacen de los libros ayudan a potenciales compradores a la hora de tomar la decisión de compra.

La debilidad de las reseñas reside en que cualquier

usuario puede escribirlas de forma anónima, por lo que acciones de uso fraudulento apoyándose en este sistema pueden darse con cierta asiduidad.

En 2004, el sistema de calidad de Amazon detectó que autores de cierto prestigio, con libros de éxito a la venta en el portal, y apoyándose en el anonimato, escribieron sus propias reseñas “autoañadiéndose” la máxima puntuación que se puede asignar a una publicación: 5 estrellas ⁷.

Tanto en el ejemplo de eBay como en el de Amazon, lo más probable es que el uso de los módulos anteriormente descritos beneficie y ayude a tener tasas de éxito más elevadas en los procesos de compra-venta. Sin embargo, a pesar de la cada vez más creciente sofisticación de estos módulos -con criterios de seguridad cada vez más estrictos-, el uso fraudulento de los mismos siempre está presente, aunque este tipo de acciones sean las menos probables.

Conclusiones

La mayoría de los actos fraudulentos son provocados por usuarios expertos, que conocen bien como funciona la web. Muchas de las acciones que se toman para solucionar los problemas derivados del fraude son a posteriori. La atención y la alerta ante cualquier movimiento anómalo son fundamentales.

El axioma, diseñar para lo más probable y no para todo lo posible, asume que hay que definir la interfaz



:: Figura 3: Reseña bibliográfica en amazon.com

⁶ Reputation Systems: Facilitating Trust in Internet Interactions. Paul Resnick, Richard Zeckhauser, Eric Friedman y Ko Kuwabara. <http://si.umich.edu/~presnick/papers/cacm00/reputations.pdf>

⁷ Amazon Glitch Unmasks War Of Reviewers. Amy Harmo. <http://tinyurl.com/22afnm>.

para aquellas acciones más probables, las que realizan la mayoría de los usuarios. No obstante, en la lucha contra el fraude, conviene no dejar de lado esa porción de acciones menos probables que, aunque no sean realizadas por la gran mayoría, pueden llegar a perjudicar el negocio al cual se destina la web.

El diseño de interacción juega un papel importante en la prevención del uso fraudulento de una web. La detección de los parámetros que se emplean para cometer acciones fraudulentas y la forma en la que estos parámetros influyen en la interfaz deben formar parte de la actividad del diseñador de interacción.



Juan Leal es licenciado en Ergonomía, especializado en Sistemas de Información, por la Universidad Técnica de Lisboa. También diplomado en Educación. Actualmente es director de usabilidad de Idealista.com, en Madrid. Ha trabajado como diseñador de interacción en Terra Networks y en IconMedialab Lisboa.

