Symantec | Website Security Solutions

Norton SECURED powered by Symantec

¿Hasta qué punto es importante la confianza a la hora de comprar por Internet?

Informe de Symantec

La importancia de la confianza en las compras por Internet

«La confianza es la clave de todo lo que hacemos en el mundo digital», *afirma Gartner.*[1]

Las gente necesita confiar en los sitios web que visita y en las empresas con las que se relaciona, y quiere saber si sus datos personales están protegidos y son tratados correctamente.

Ante todo, necesita tener la certeza de que las empresas hacen todo lo posible para protegerse de los ciberdelincuentes y de sus sofisticados ataques, encaminados a socavar la economía en Internet para obtener beneficios ilícitos.

La batalla por la confianza en línea

Nadie duda de que la confianza de los compradores es imprescindible en Internet, pero ¿qué hacen las empresas para fomentarla?

Recientemente, Symantec encargó a la empresa de investigación de mercado YouGov una encuesta para conocer hasta qué punto preocupa a los compradores la cuestión de la seguridad, y si los distintivos de seguridad de los sitios web influyen en la decisión de comprar por Internet. La encuesta recabó las opiniones de internautas del Reino Unido, EE. UU., Francia y Alemania.

Los resultados fueron concluyentes: a la gente le preocupa la seguridad a la hora de comprar por Internet, pero la mayoría ya sabe en qué debe fijarse para protegerse.

A las empresas se les suele recomendar que utilicen certificados SSL con Extended Validation, que controlen la fecha de caducidad de los certificados SSL y que exhiban distintivos de confianza en sus sitios web, pero ¿realmente reparan los compradores en todos esos elementos?

Nuestra encuesta revela que sí

Los usuarios se sienten más seguros realizando transacciones en los sitios web en los que confían, y esos elementos les sirven para determinar la fiabilidad de un sitio web.

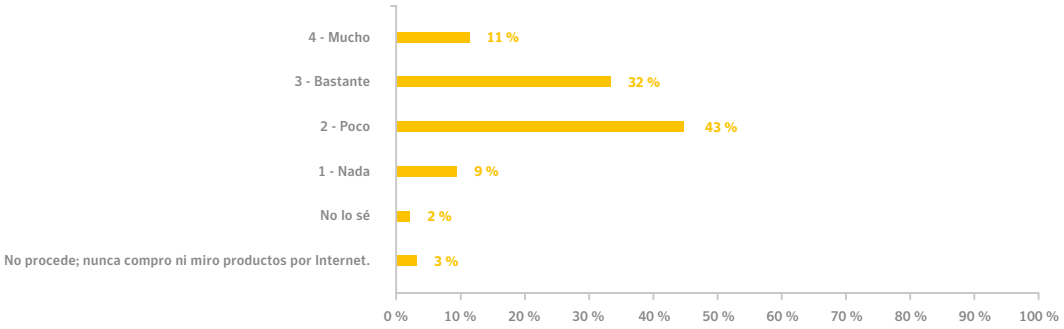
Dicho de otro modo, las empresas que no mantienen la seguridad del sitio web no infunden confianza a los clientes. Y sin confianza, ya pueden decir adiós a las ventas.

1. NetworkComputing: «Expired Digital Certificates: A Management Challenge» (http://www.networkcomputing.com/networking/expired-digital-certificates-a-management-challenge/d/d-id/1102269).

Todas las cifras pertenecen a YouGov Plc., a menos que se indique lo contrario. El tamaño total de la muestra fue de 7541 adultos: 2102 en el Reino Unido, 1011 en Francia, 2050 en Alemania y 2378 en Estados Unidos. El trabajo de campo se realizó entre el 3 y el 8 de septiembre de 2015. La encuesta se llevó a cabo por Internet. Las cifras se presentan como datos ponderados y son representativas de la población adulta (personas mayores de 18 años en todos los mercados).

La preocupación de los clientes

P1 Al comprar o mirar productos por Internet, ¿hasta qué punto le preocupa, en general, la cuestión de la seguridad (fraude con tarjetas de crédito, usurpación de identidad, etc.)?



Muestra: Personas adultas con acceso a Internet (7541)

Está claro que a mucha gente le preocupa la seguridad a la hora de comprar por Internet. En nuestro estudio, el 43 % de los encuestados declaró sentirse muy o bastante preocupado, y apenas un 9 % declaró no sentirse nada preocupado.

Los propietarios de los sitios web deben aceptar el hecho de que la confianza y la seguridad son importantes para los consumidores. Obviamente, factores como el precio, la calidad de los productos y la experiencia de usuario también influyen, pero la seguridad es un factor que no se debe pasar por alto.

Concretamente, una quinta parte de la gente que compra o mira productos por Internet manifiesta sentirse preocupada por el robo de datos bancarios, y prácticamente otros tantos (19 %) afirman sentirse preocupados por las usurpaciones de identidad (una cifra que en EE. UU. se dispara al 36 % de los encuestados). Por tanto, existe cierta inquietud en torno a la seguridad de los datos que facilitan los clientes y a la credibilidad de los receptores de dichos datos.

De ahí la importancia de utilizar certificados SSL/TLS fiables emitidos por autoridades de certificación de reconocido prestigio, como es el caso de Symantec. Los certificados se encargan de cifrar los datos personales y bancarios y de verificar la identidad del propietario del sitio web, las dos principales preocupaciones de los compradores.

Hay motivos para preocuparse

La preocupación de los usuarios es comprensible: en 2014, cada segundo se perdieron o robaron 32 registros de datos,[2] y el 80 %[3] de las usurpaciones de identidad durante los tres primeros meses de 2015 se perpetraron o intentaron en línea.

2. Nasdaq: «Credit card fraud and ID theft statistics» (http://www.nasdaq.com/article/credit-card-fraud-and-id-theft-statistics-cm520388#ixzz3mZTIPqsa).
3. BBC News: «Number of identity theft victims 'rises by a third'» (http://www.bbc.co.uk/news/uk-32890979).

La razón de que estas cifras sean tan altas es muy simple: los datos personales son valiosos para los ciberdelincuentes. El informe más reciente de Symantec sobre amenazas de seguridad en Internet[4] denuncia que el valor en el mercado negro de los datos de las tarjetas de crédito oscila entre los 0,50 y 20 dólares y que, en función del grado de detalle, la información sobre la identidad se cotiza a entre 10 y 50 dólares.

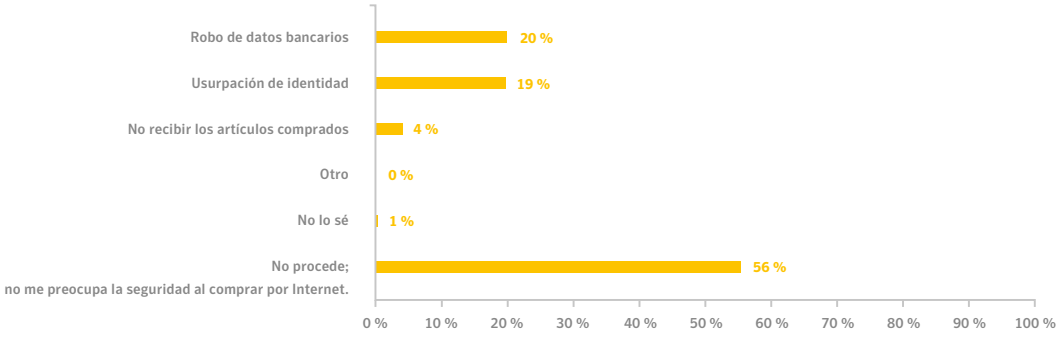
Los casos de robo de datos y fraudes con tarjetas de crédito no son las únicos que generan esta desconfianza. La cobertura mediática de los casos más sensacionales de ciberdelincuencia también contribuye a crear un clima de ansiedad entre los consumidores.

Un ejemplo perfecto es el reciente ataque sufrido por Ashley Madison, con casos de suicidios y escándalos de famosos de por medio que añaden morbo a un incidente ya fascinante de por sí contra el sitio web de citas extramatrimoniales.

Si a eso sumamos fallos de seguridad tan graves como el sufrido a principios de este año por la Oficina de Administración de Personal de Estados Unidos,[5] que afectó a los datos personales de casi cuatro millones de empleados del gobierno, es fácil prever que los temores irán en aumento. Si la gente no puede confiar siquiera en la ciberseguridad de su propio gobierno, no parece probable que otorguen su confianza a una web de comercio electrónico sin argumentos de peso.

Despreocupación no es sinónimo de desconocimiento

P2 Ha dicho que le preocupa la seguridad al comprar por Internet. ¿Qué es lo que más le preocupa? (Seleccione la opción que le parezca más importante.)



Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).

Si bien hay personas que se muestran preocupadas por aspectos concretos de la seguridad de las compras en Internet, el 56 % de los encuestados manifiestan no sentir ninguna preocupación. En cualquier caso, esto no significa que no les importe la seguridad.

Tal como se explica más adelante en este informe, hay un porcentaje sorprendentemente alto de usuarios que buscan señales dignas de credibilidad y confianza, como la indicación «https» o el icono del candado en la barra de direcciones. Es probable que el elevado número de encuestados que afirman no sentirse preocupados lo hagan precisamente porque son conscientes de los riesgos y porque saben cómo evitarlos.

4. Symantec. 2015 Internet Security Threat Report, Volume 20 - http://www.symantec.com/security_response/publications/threatreport.jsp
5. BBC News. Millions of US government workers hit by data breach - http://www.bbc.co.uk/news/world-us-canada-33017310

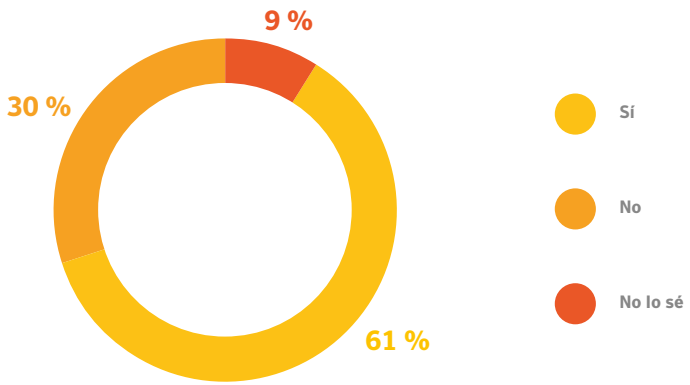
La importancia de una dirección de confianza

En la vida real, el lugar donde se encuentra físicamente un negocio es un factor determinante para su credibilidad. Pensemos en las tiendas de la calle Serrano de Madrid, los diseñadores de la Quinta Avenida de Nueva York o prácticamente todos los comercios de los Campos Elíseos de París. Cuando uno entra en cualquiera de esos establecimientos, sabe lo que va a encontrar.

Lo mismo sucede en la Internet: el aspecto de la dirección URL dice mucho de un negocio y determina la percepción que tienen de él los clientes.

Hemos preguntado a nuestros encuestados si, en general, tienden a fijarse en la barra de direcciones del navegador cuando compran algún artículo por Internet. La respuesta sorprenderá a muchos:

Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).



Casi dos tercios de los usuarios se fijan la dirección URL cuando compran por Internet para saber si el sitio web es seguro. Veamos qué buscan exactamente.

Principales indicadores de confianza:

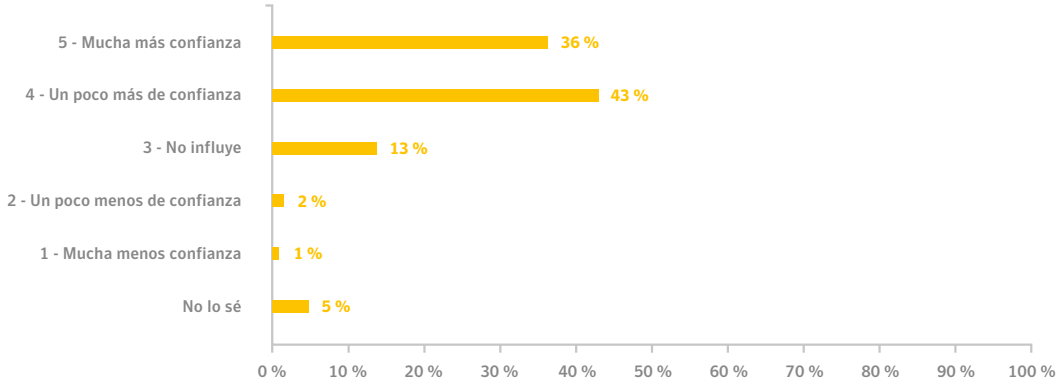
- **El prefijo «https»** (en lugar de «http», sin cifrado) al principio de la dirección indica que toda la información que se envíe al sitio web estará cifrada y que, por tanto, los ciberdelincuentes no podrán espiarla.
- **El candado gris** indica al visitante que la persona o empresa que dirige el sitio web es quien ha comprado el dominio, pero sin confirmar quién es el propietario.
- **El candado verde** revela que el sitio web utiliza SSL con Extended Validation, lo que implica que el propietario del sitio web se ha sometido a un riguroso control de identidad para confirmar que es quien dice ser, que dirige el sitio web y que es su propietario.

¿Son efectivos los indicadores de confianza?

Mostramos a los encuestados una barra de direcciones con un candado:

Acto seguido, les preguntamos si el hecho de que aparezca el candado les daba más o menos confianza a la hora de comprar por Internet.

Un sorprendente 78 % (redondeando decimales) manifestó que les daba más confianza.



Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).

El candado verde del ejemplo indica que el sitio web utiliza SSL con Extended Validation, que aumenta la confianza del cliente no solo en el sitio web, sino también en el negocio.

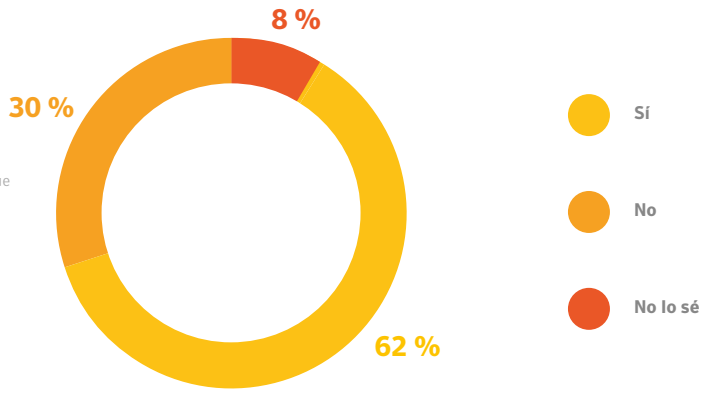
La conclusión es clara: cuando se trata de infundir confianza y credibilidad, los certificados SSL con Extended Validation son un requisito indispensable.

Tasa de conversión: la edad influye

«La clave para fidelizar a un comprador para toda la vida es ganarse su confianza desde el principio», sostiene Nielsen.[6]

Efectivamente, de la encuesta se desprende que la confianza es esencial para garantizar una alta tasa de conversión en todos los grupos poblacionales. A la pregunta de si alguna vez habían abandonado un proceso de compra por no confiar en el sitio web, la respuesta fue prácticamente unánime en todas las franjas de edad (y en todas las regiones, de hecho).

Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).



Es preciso infundir confianza a los clientes de todas las edades, o de lo contrario será muy difícil lograr una buena tasa de conversión. Eso sí, la forma de infundir confianza debe adaptarse a las características específicas de cada grupo.

Los jóvenes

El reciente informe de Nielsen, titulado *Ecommerce: evolution or revolution*,[6] revela que «los jóvenes de la llamada "generación del milenio" (un 53 % de los encuestados) tienen previsto hacer alguna compra por Internet en todas las categorías de productos del estudio».

Los *millenials* no solo conforman el grueso de los compradores online, sino que, tras analizar la conducta de compra de cada categoría, el estudio de Nielsen también sugiere que un comprador online lo es para toda la vida.

Ganarse la confianza de los consumidores a una edad temprana puede ser una inversión muy lucrativa de cara al futuro, de ahí la importancia de saber cómo atraer el interés de los compradores más jóvenes.

6. Nielsen: E-Commerce: Evolution or revolution in the fast-moving consumer goods world?, agosto de 2014 (http://ir.nielsen.com/files/doc_financials/Nielsen-Global-E-commerce-Report-August-2014.pdf).

Mostramos a los encuestados cuatro imágenes:

La imagen 1

La imagen 2

- **La imagen 1** muestra un sitio web fiable que utiliza SSL con Extended Validation (nótese la barra de direc ciones de color verde y el prefijo «https»).
- **La imagen 2** no contiene ningún indicador de seguridad.

Los certificados SSL con Extended Validation son importantes y para reconocerlos se necesita un cierto nivel de conocimientos técnicos. Más de dos tercios (70 %) de los encuestados de entre 18 y 24 años señalaron que la imagen 1 era el sitio web que más confianza les transmitía.

Los más jóvenes son los que más saben de seguridad en Internet. No se les escapa qué elementos visuales determinan si un sitio web es fiable o no. Por tanto, el mejor argumento para mejorar la tasa de conversión de este grupo es la transparencia.

La empresa debe dejar constancia de que ha tomado todas las medidas posibles para demostrar su credibilidad y proteger los datos de los usuarios. Esto implica:

- **SSL con Extended Validation,** que hace que la barra de direcciones aparezca de color verde.
- **Marcas de confianza,** como el sello Norton Secured, colocadas en un lugar bien visible para que no haya dudas de quién es el garante de la confianza en el sitio web.
- **Tecnología SSL Always-On,** para cifrar todas las interacciones del cliente con el sitio web al comprar o interesarse por algún artículo.

Los no tan jóvenes

Las previsiones de Euromonitor[7] apuntan a que, en 2020, el poder adquisitivo de las personas de más de 60 años de todo el mundo será de 15 billones de dólares. Además, la imagen estereotipada del abuelo que se las ve y se las desea para encender el ordenador ha pasado a la historia.

Según Business Insider Intelligence, «un porcentaje elevadísimo de consumidores de mediana edad está comprando por Internet». En Estados Unidos, una de cada cuatro personas que compran en Internet con dispositivos móviles tiene más de 55 años. «Con el paulatino envejecimiento de la población, cada vez habrá un mayor porcentaje de consumidores conectados e Internet seguirá cobrando protagonismo», vaticina John Burbank, presidente de iniciativas estratégicas de Nielsen.

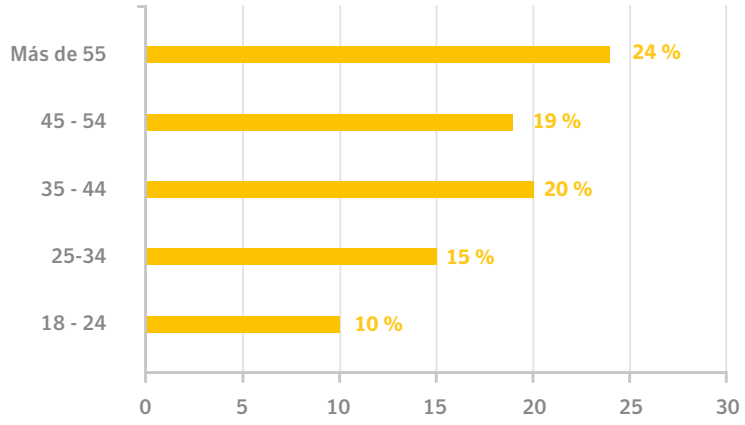
La generación de personas mayores es un grupo poblacional en rápido crecimiento, socialmente acomodado y cada vez más conocedor de la tecnología, pero que necesita más información e indicadores menos técnicos que la gente joven.

Un grupo de compradores preocupados

Volviendo a nuestra encuesta, el 48 % de los encuestados mayores de 55 años declaró sentirse preocupado por los problemas de seguridad de las compras por Internet, frente a solo el 34 % de los jóvenes de entre 18 y 24 años.

En la misma línea, al preguntarles qué era lo que más les preocupaba al comprar por Internet, pudimos constatar que, de media, a mayor edad, mayor es la preocupación que sienten los usuarios por las usurpaciones de identidad.

Porcentajes de encuestados que eligieron la usurpación de identidad como principal motivo de preocupación.



Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).

Asimismo, los compradores de mayor edad son los que menos conocimientos técnicos poseen. Al mostrarles las mismas dos imágenes que a los jóvenes de 18-24 años (una con SSL con Extended Validation y la otra sin ningún distintivo de seguridad), solo el 29 % de los mayores de 55 años eligieron la imagen de SSL con Extended Validation como el sitio web que a ellos les inspiraba mayor confianza.

7. Financial Times: «The Silver Economy: Baby boomers power new age of spending», 7 de noviembre de 2014 (http://www.ft.com/cms/s/0/e9fc95c0-44b1-11e4-ab0c-00144feabdc0.html#axzz3mZB73kbn).

Las empresas necesitan una manera más sencilla de demostrar su credibilidad ante este grupo de compradores, y la encuesta sugiere que las marcas de confianza son la solución ideal.

A los encuestados se les formuló esta pregunta:
Imagine que está a punto de comprar un artículo por Internet. De las siguientes imágenes, ¿qué sitio web le merece más confianza?

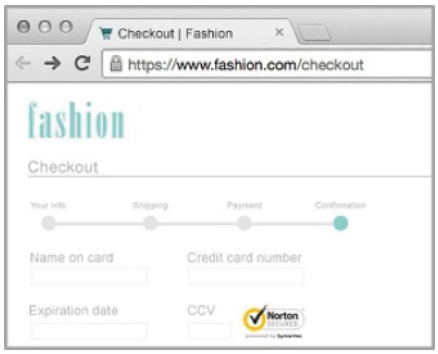
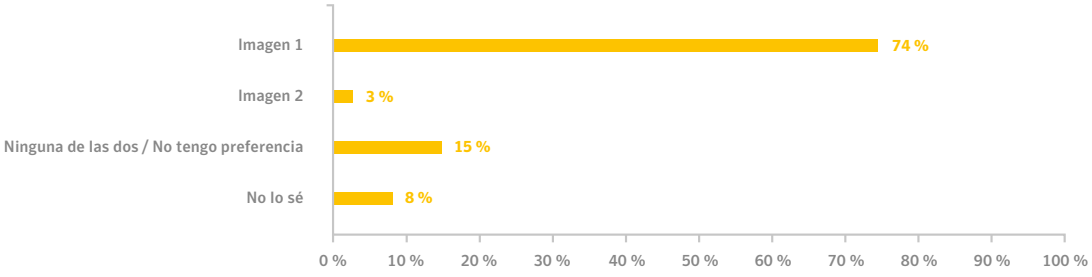


Imagen 1

Imagen 2

Casi tres cuartas partes (74 %) eligieron la imagen 1, la que incorporaba el sello Norton Secured. Esta preferencia se repitió en todas las franjas de edad.



Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).

La conclusión es que las empresas, para infundir confianza por igual en todas las franjas de edad, necesitan certificados SSL con Extended Validation y la marca de confianza a modo de refuerzo.

La eficacia de las marcas de confianza

Como se ha visto, con independencia del mercado objetivo, la presencia del sello Norton Secured aumenta considerablemente la probabilidad de que el cliente confíe en un sitio web para realizar sus compras.

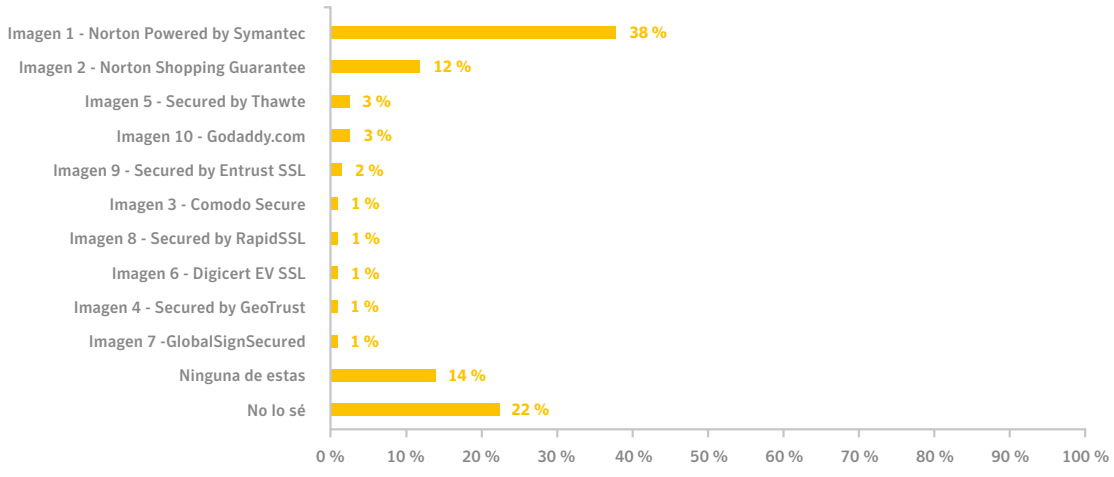
Esas marcas de confianza se pueden colocar en cualquier lugar del sitio web, aunque diversos estudios revelan que son más efectivos si se ponen junto a los campos más sensibles de un formulario. En un experimento[8] se hizo la prueba de quitar la marca de confianza de la parte superior de la página y ponerla junto al formulario, y la tasa de conversión aumentó un 6 %.

El nombre importa

La eficacia de la marca de confianza no depende solo del lugar donde esta aparece; el nombre también influye.

La marca de confianza certifica que una empresa externa ha verificado el sitio web y le otorga su confianza para dar seguridad al usuario. Por tanto, la opinión de una empresa reconocida y con buena reputación siempre tendrá más valor para el visitante que otra empresa de la que no haya oído hablar nunca.

Hemos preguntado a nuestros encuestados qué marca les merecería más confianza a la hora de comprar por Internet. (Las marcas de confianza se presentaron en orden aleatorio.)



Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).

8. Conversion Voodoo: «Proper placement of you 'trust logos' will improve conversion rates» (http://www.conversionvoodoo.com/blog/2012/05/proper-placement-of-your-trust-logos-will-improve-your-conversion-rate/)

La credibilidad de Symantec no admite discusión: casi la mitad (49 %) de los encuestados eligió una de las dos marcas de confianza de Symantec: Norton Secured Seal y Norton Shopping Guarantee.

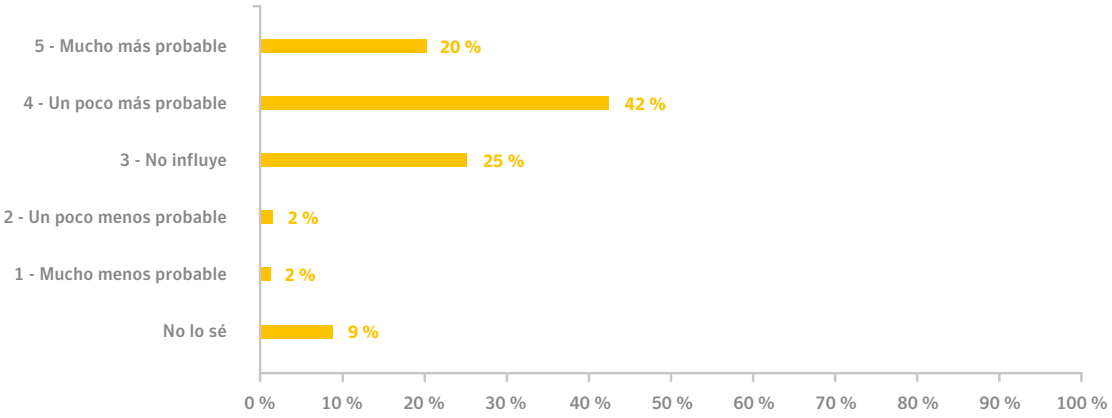
Aunque la confianza es un factor determinante para las tasas de conversión, no siempre es sinónimo de compra. Por eso, decidimos comprender mejor la correlación que existe entre una marca de confianza de Symantec y una transacción completada.

Enseñamos a los encuestados el sello Norton Secured, un distintivo que aparece diariamente más de 500 millones de veces en los sitios web de 170 países.

Norton™ SECURED
powered by Symantec

Acto seguido, les preguntamos si sería más probable que completasen una transacción (o compra) si ven un distintivo como este en la página donde se consignan los datos bancarios.

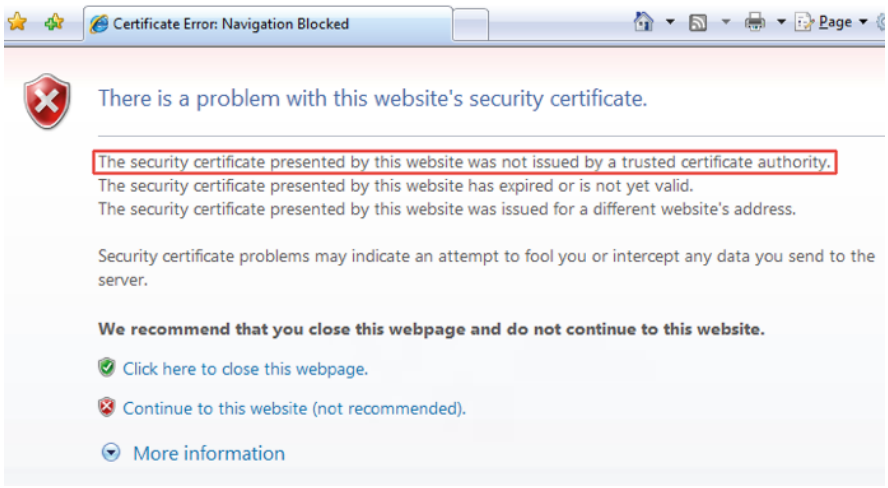
Casi dos tercios (el 63 %, redondeando decimales) manifestó que sería más probable.



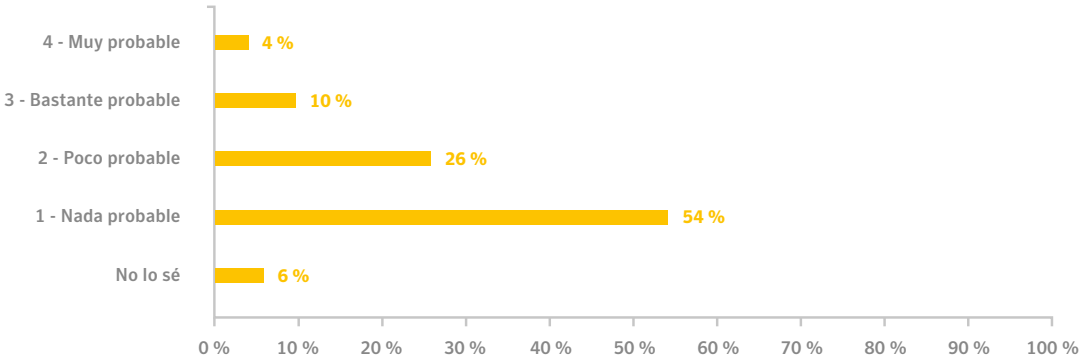
Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).

¿Qué pasa si la empresa no está pendiente? La reacción de los consumidores frente a las advertencias de seguridad

Ganarse la confianza de los consumidores es importante, pero luego hay que esforzarse por mantenerla. Cuando un certificado SSL caduca y no se renueva, los visitantes se encontrarán con una advertencia de seguridad como esta:



Preguntamos a nuestros encuestados cuál sería la probabilidad de que continuaran en un sitio web a la vista de esta advertencia. Los resultados revelan que, en la mayoría de los casos, este tipo de advertencias merma la confianza: hasta un 80 % considera muy poco probable que continuasen en el sitio web.



Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).

Al igual que en otros apartados, a mayor edad del encuestado, mayor es la probabilidad de que abandone el sitio web. Dos tercios de los compradores mayores de 55 afirmaron que abandonarían el sitio web, mientras que, en el caso de los jóvenes de entre 18 y 24 años, la cifra se redujo al 41 %.

El efecto negativo que tienen las advertencias de seguridad en la credibilidad de un sitio web no es ninguna sorpresa. No solo están pensadas para eso —avisar a los visitantes de que no tienen por qué confiar en el sitio web—, sino que además un estudio[9] realizado por la Universidad de California (Berkeley) confirma que los usuarios las tienen muy en cuenta:

Durante nuestro estudio de campo, los usuarios decidieron continuar tras una de cada diez advertencias de malware y phishing *en Mozilla Firefox, una de cada cuatro advertencias de malware y phishing en Google Chrome y una de cada tres advertencias de SSL en Mozilla Firefox. Esto demuestra que, en la práctica, las advertencias de seguridad pueden ser eficaces.*

El propietario o responsable de seguridad de un sitio web debe optimizar la administración de certificados SSL para llevar un control riguroso de todos ellos. Recibir un aviso a tiempo con las fechas de caducidad puede ser la diferencia entre ganar un cliente o perder varios.

De la cita anterior también se desprende que conviene analizar continuamente el sitio web en busca de vulnerabilidades y malware, ya que las advertencias de malware suelen resultar muy disuasorias. Paralelamente, los buscadores cada vez analizan más sitios web en busca de malware y bloquean los sitios web infectados. Esto puede tener efectos catastróficos en el tráfico procedente de los resultados orgánicos de las búsquedas.

9. Usernix: «Alice in Warningland: A large scale field study of browser security warning effectiveness» (https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe).

Rasgos propios de cada país

Aunque la mayor parte de este informe presenta una serie de resultados combinados que YouGov ha obtenido a partir de las opiniones recabadas en el Reino Unido, Alemania, Francia y EE. UU., en Europa se dan algunas variaciones que vale la pena destacar.

Reino Unido: muy concienciados con la seguridad

«La seguridad en Internet es la base de toda la economía digital. La necesitamos para proteger a nuestras empresas, ciudadanos, servicios públicos... En el Reino Unido, la confianza en la seguridad de Internet es crucial para los consumidores, empresas e inversores.»

Así se expresaba Ed Vaizey, ministro del Reino Unido encargado de la economía digital.[10] Es evidente que en se trata de un país donde existe un gran interés por la seguridad y por educar a los consumidores.

A la pregunta de hasta qué punto les preocupa la seguridad del comercio electrónico, el Reino Unido fue el país donde menos encuestados manifestaron sentirse muy preocupados: apenas el 4 %. De hecho, casi dos tercios (63 %) afirmaron que se sentían poco o nada preocupados, una cifra muy superior la cifra combinada del 52 %.

Esto se debe probablemente a que los consumidores británicos, gracias a campañas públicas como «Get Safe Online», tienen más claro en qué deben fijarse para determinar si un sitio web es seguro o no. También son los que más dudarían en seguir visitando un sitio web tras recibir una advertencia de seguridad: solo un 11 % respondió que sería muy probable o bastante probable que lo hicieran.

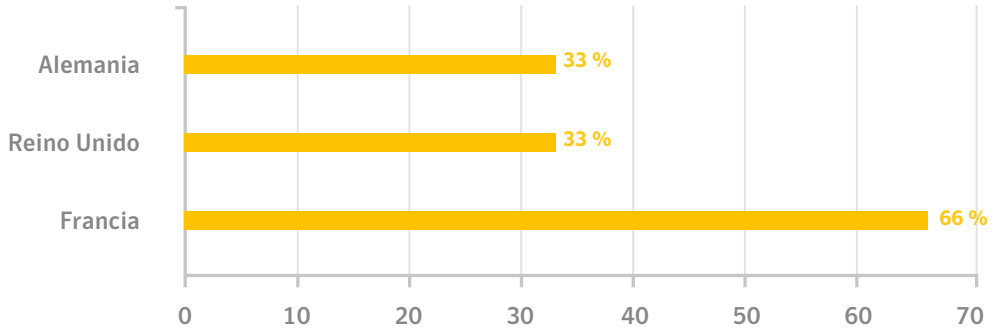
Al mostrarles la barra de direcciones con el candado, el 43 % respondió que esto les daría mucha más confianza para completar una compra en línea, una cifra muy superior a la cifra combinada global del 36 %.

10. ComputerWeekly.com: «Majority of UK business have been targeted by cyber criminals.» (http://www.computerweekly.com/news/4500253942/Majority-of-UK-businesses-have-been-targeted-by-cyber-criminals).

Francia: los compradores inquietos

Los encuestados franceses fueron, con diferencia, los que mostraron una mayor preocupación por la cuestión de la seguridad. Dos tercios admitieron que les generaba bastante o mucha preocupación, un resultado que contrasta con el porcentaje combinado del 43 %.

Porcentaje de encuestados que manifestó sentirse muy o bastante preocupado por la seguridad de las compras en Internet



Muestra: Personas adultas que alguna vez han comprado o mirado artículos por Internet (7330).

La mitad de los encuestados franceses manifestó que su mayor preocupación era el robo de datos bancarios; en las cifras combinadas la proporción fue mucho menor: una quinta parte.

A pesar de ello, los galos se mostraron más dispuestos a seguir en un sitio web tras recibir una advertencia de seguridad. Más de una cuarta parte (26 %) respondió que sería muy o bastante probable que continuara, mientras que la cifra combinada se situaba en apenas un 14 %.

Desde luego, si visitan sitios web con certificados SSL caducados o revocados, no les faltan motivos para estar preocupados.

Alemania: los más difíciles de convencer

Los resultados de la encuesta sugieren que los consumidores alemanes son los que menos importancia otorgan a los indicadores de confianza.

Por ejemplo, solo una cuarta parte de los encuestados declaró que el candado verde en la barra de direcciones le daría mucha más confianza para completar un proceso de compra. En el Reino Unido y Francia, en cambio, esa respuesta fue elegida por el 43 % de los encuestados.

Del mismo modo, cuando se les mostraron las dos imágenes, una de un sitio web con «https», candado y sello Norton Secured, y la otra de un sitio web sin ningún indicador de confianza, apenas dos tercios de los encuestados respondieron que la primera era la que les merecía más confianza para comprar por Internet y un 21 % respondió que no tenía preferencia por ninguna en particular. Los resultados combinados fueron del 74 % y el 15 %, respectivamente.

Un estudio publicado por el German Institute for Trust and Security on the Internet (Instituto Alemán para la Confianza y la Seguridad en Internet)[11] confirma que la confianza del público alemán en Internet se ha deteriorado notablemente. Esto explicaría el porqué de la escasa aceptación de ciertos indicadores de seguridad en nuestra encuesta.

Por otro lado, en el informe State of IT Security in Germany 2014 (Estado de la seguridad informática en Alemania 2014)[12], que publica la Oficina Federal Alemana para la Seguridad de la Información, se afirma lo siguiente:

«A pesar de la mayor concienciación [por la seguridad] y de la pérdida de confianza [en Internet], las cifras revelan que son muy pocos los que están adoptando medidas para mejorar la seguridad.»

Es posible que los consumidores alemanes no hayan tenido ocasión de informarse sobre los elementos visuales que garantizan la seguridad al comprar por Internet.

Ciertamente, las empresas alemanas lo tienen difícil para establecer una relación de confianza con su clientela potencial. Un cambio reciente de la legislación[13], que establece una sanción para aquellos propietarios de sitios web alemanes que no mantengan actualizada la seguridad del sitio web, tal vez contribuya a aliviar el problema, pero en cualquier caso el verdadero reto seguirá siendo cómo garantizar la credibilidad y la seguridad.

11. DIVSI: «PRISM und die Folgen: Sicherheitsgefühl im Internet verschlechtert», 3 de julio de 2013 (https://www.divsi.de/prism-und-die-folgen-sicherheitsgefuehl-im-internet-verschlechtert/).

12. Federal Office for Information Security: *The State of IT Security in Germany 2014* (https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2014_pdf.pdf?__blob=publicationFile).

13. Friedrich Graf von Westphalen & Partner: «German Bundestag passes IT Security Act» (http://www.fgvw.de/2704-1-German+Bundestag+passes+IT+Security+Act.html).

Symantec le ayuda a ganarse la confianza de sus clientes

Symantec es líder mundial en seguridad de sitios web, con más de un millón servidores web protegidos en todo el mundo. Symantec SSL proporciona soluciones de seguridad al 91 % de las empresas de la lista Fortune 500.

Ofrecemos una gama de productos y servicios que ayudarán a su empresa a establecer una relación de confianza con sus clientes y mejorar las tasas de conversión.

El producto	Qué es	Cómo genera confianza
Certificados SSL/TLS de Symantec	Ofrecemos una serie de certificados SSL que le ayudarán a proteger sitios web internos o externos	Los certificados SSL confirman quién es el propietario de un sitio web y garantizan que los datos que el visitante intercambia con el servidor web están cifrados para impedir que los ciberdelincuentes puedan espiarlos.
SSL con Extended Validation	Llevamos a cabo una rigurosa verificación de la identidad del negocio para garantizar que el propietario es quien dice ser, y que el negocio está registrado en los organismos oficiales competentes.	SSL con Extended Validation hace que la barra de direcciones del navegador se vuelva de color verde o muestre un candado de color verde. Esta tecnología garantiza al cliente que el propietario del sitio web es quien dice ser y que se trata de una empresa con buena reputación.
Sello Norton Secured	Tal como se muestra en el informe, esta marca de confianza indica que el sitio web está protegido con la tecnología SSL de Symantec.	De esta forma, los visitantes saben que una empresa externa con buena reputación ha depositado su confianza en su sitio web. Nuestra encuesta revela que los clientes reaccionan positivamente cuando ven este sello en un sitio web, y estudios previos han demostrado que es la marca de confianza con más prestigio en Internet.
Seal-in-Search	En los navegadores con ciertos complementos de seguridad, muestra el sello Norton Secured junto al sitio de Internet en los resultados de las búsquedas, en las tiendas de comercio electrónico asociadas y en los sitios webs de análisis de productos.	Es una forma de ganarse la confianza del cliente antes incluso de que visite el sitio web para que haga clic en ese enlace de la página de resultados del buscador, en lugar de elegir otro enlace de la competencia.

El producto	Qué es	Cómo genera confianza
Norton Shopping Guarantee	Proporciona tres garantías a los clientes, válidas durante 30 días: • Protección frente a la usurpación de identidad, de hasta 10 000 dólares. • Garantía completa de terceros para las condiciones de venta, de hasta 1000 dólares. • Precio mínimo garantizado, de hasta 100 dólares.	De esta forma, el cliente tiene la certeza de que el propietario confía plenamente en su propio sitio web y de que no saldría perdiendo en ningún caso.
Análisis de vulnerabilidades y malware	Ciertos certificados SSL de Symantec incluyen automáticamente y de forma gratuita análisis semanales de vulnerabilidades y escaneados diarios de malware.	En 2014, el 75 % de los sitios web[4] escaneados presentó vulnerabilidades, muy graves en una quinta parte de los casos. La desprotección contra el malware pone a los clientes en una situación de riesgo y aumenta las posibilidades de que aparezcan las advertencias de seguridad en el sitio web. Una manera de evitarlo es mediante análisis periódicos.
Detección y automatización	Las herramientas de detección y automatización de Symantec facilitan el control de los certificados SSL, comprueban que el sitio web no contiene certificados fraudulentos y garantizan que todos los certificados han sido emitidos por una autoridad de certificación homologada. Asimismo, avisan de las fechas de caducidad de los certificados SSL con suficiente antelación.	Como se ha visto, los certificados SSL caducados merman la confianza de los clientes. Cuando una empresa crece resulta más difícil llevar el control de todos los certificados SSL, con el consiguiente riesgo de que caduquen por descuido. Las herramientas de Symantec ayudan a evitar esta situación.

Si desea obtener más información acerca de cómo infundir confianza a sus clientes de la mano de un proveedor de seguridad en Internet de prestigio mundial, póngase en contacto con Symantec.

4. Symantec. 2015 Internet Security Threat Report, Volume 20 - http://www.symantec.com/security_response/publications/threatreport.jsp

Symantec | Website Security Solutions

Norton SECURED powered by Symantec

Si desea más información,
visite nuestro sitio web
www.symantec.es/ssl

Para contactar con un especialista en productos
900 93 1298 o al **+353 1 793 9076.**

Sobre Symantec
Symantec es líder mundial en soluciones de gestión de sistemas, almacenamiento y seguridad. Su objetivo es ayudar a empresas y particulares a gestionar y proteger sus datos en un mundo cada vez más dominado por la información. Nuestros servicios y programas garantizan una protección más completa y eficaz frente a una mayor cantidad de riesgos, lo que es sinónimo de tranquilidad sea cual sea el medio donde se utilice o almacene la información.

Symantec
Symantec Spain S.L.
Parque Empresarial La Finca – Somosaguas
Paseo del Club Deportivo, Edificio 13, oficina D1, 28223
Pozuelo de Alarcón, Madrid, España

¿Hasta qué punto es importante la confianza a la hora de comprar por Internet?