Comercio electrónico y ciberseguridad en España:

Lo que cada comprador y empresa debe saber antes de que sea tarde

110.000 millones de euros en juego, 3 de cada 10 usuarios ya víctimas de fraude. Esta no es una advertencia genérica: es el diagnóstico de un ecosistema en el que participas cada vez que haces clic en "Comprar ahora".

Un mercado inmenso con un talón de Aquiles enorme

España ha construido uno de los ecosistemas de comercio electrónico más dinámicos de Europa. Con ventas que superan los 110.000 millones de euros, el e-commerce nacional no es una tendencia emergente: es ya una columna vertebral de la economía. Y como ocurre con todo lo que tiene valor, se ha convertido en un objetivo prioritario para quienes viven de explotar vulnerabilidades.

Lo que hace especialmente compleja esta situación es la paradoja que los datos revelan: el 72% de los consumidores españoles declara sentirse en riesgo cuando compra online por la forma en que sus datos son recopilados y tratados. Sin embargo, el comercio digital sigue creciendo. Compramos a pesar del miedo. Eso no habla de irresponsabilidad; habla de que el mercado digital se ha vuelto tan necesario que renunciar a él ya no es una opción real.

El problema es que esa necesidad, combinada con una cultura de seguridad todavía insuficiente, crea el terreno perfecto para el fraude. Y los números lo confirman: 3 de cada 10 usuarios en España ya han sufrido algún tipo de fraude digital en sus compras online. No hablamos de una minoría técnicamente inexperta. Hablamos de cualquiera.

"En 2026, el mayor activo del comercio electrónico no es el catálogo ni el precio. Es la confianza digital. Y esa confianza se gana con seguridad real, no con apariencia de seguridad."

El fraude digital no es un error técnico: es un diseño

Existe un malentendido muy extendido que conviene desmontar desde el principio: los ciberataques contra compradores y tiendas online no se producen porque alguien cometió un error técnico. Se producen porque están diseñados para explotar algo mucho más difícil de parchear que un software desactualizado: el comportamiento humano.

El phishing —el intento de suplantar la identidad de una empresa o institución para robar credenciales o datos bancarios— sigue siendo la puerta de entrada más común.

En el contexto del e-commerce, se materializa en correos que imitan a la perfección la comunicación de plataformas como Amazon, El Corte Inglés Digital o Correos, informando de un problema con tu pedido o un pago fallido. El enlace te lleva a una réplica de la web original. Introduces tus datos. Y los pierdes.

Lo que ha cambiado en los últimos dos años es la sofisticación. La inteligencia artificial generativa permite producir mensajes de phishing sin los errores ortográficos que antes los delataban, personalizados con información real extraída de fuentes públicas —técnica conocida como OSINT (Open Source Intelligence)— y adaptados al tono exacto de cada empresa imitada. El resultado es un engaño que ni los usuarios más precavidos detectan a primera vista.

La economía del dato como motor del riesgo

Detrás de cada transacción de comercio electrónico hay una infraestructura de datos que pocos compradores visualizan: nombre, dirección, método de pago, historial de compras, dispositivo utilizado, geolocalización aproximada. Toda esa información tiene un valor en mercados negros digitales que va mucho más allá del importe de la compra.

Cuando una plataforma sufre una brecha de seguridad, lo que se filtra no son solo tarjetas de crédito: se filtra contexto. Y el contexto —saber que alguien compra frecuentemente en una categoría concreta, que vive en un barrio determinado, que usa habitualmente ciertos dispositivos— es combustible para ataques de ingeniería social mucho más precisos en el futuro.

El 72% de consumidores que se siente en riesgo por la recopilación de datos no está siendo paranoico. Está siendo, quizá sin saberlo, bastante preciso en su diagnóstico.

Lo que las empresas están haciendo (y lo que aún falta)

La respuesta del sector al incremento del fraude ha sido real y medible. Las empresas de comercio electrónico han intensificado la adopción de capas de seguridad que hasta hace pocos años eran excepcionales y hoy se están convirtiendo en estándar.

Cifrado HTTPS y autenticación reforzada

El protocolo HTTPS, que garantiza que la comunicación entre el navegador del usuario y el servidor de la tienda viaja cifrada, es hoy prácticamente universal en plataformas serias. Pero el HTTPS solo protege el canal: no garantiza que quién está al otro lado sea legítimo. Por eso las empresas más avanzadas han añadido capas adicionales: autenticación de doble factor para cuentas de clientes, verificación biométrica en apps móviles y sistemas de detección de comportamiento anómalo basados en IA.

Inteligencia artificial como escudo, no solo como arma

La misma tecnología que los criminales usan para construir phishing más sofisticado, las empresas la están desplegando para detectarlo. Los sistemas de análisis de fraude en tiempo real evalúan cientos de variables en milisegundos —velocidad de escritura, dirección IP, patrón de navegación, coherencia entre datos de envío y facturación— para asignar un nivel de riesgo a cada transacción antes de que se procese.

Esto ha reducido significativamente el fraude en plataformas que han apostado por estas soluciones. El reto está en las pequeñas y medianas empresas, donde la inversión en estas herramientas sigue siendo limitada y donde, paradójicamente, la vigilancia de los atacantes es cada vez mayor.

Seguros cibernéticos: la red de seguridad que se está normalizando

Otro cambio estructural relevante es la adopción creciente de seguros cibernéticos por parte del tejido empresarial español. Ante la certeza de que ningún sistema es invulnerable al 100%, las empresas —especialmente pymes con acceso a clientes y datos sensibles— están incorporando pólizas que cubren desde los costes de respuesta ante una brecha hasta la responsabilidad frente a terceros afectados.

Este movimiento señala una madurez importante: la ciberseguridad ha dejado de ser solo un problema técnico para convertirse en una variable de gestión de riesgo empresarial.

El papel del INCIBE en el ecosistema nacional

En España, el Instituto Nacional de Ciberseguridad (INCIBE) juega un rol central en la arquitectura de protección del comercio digital. A través de sus líneas de ayuda, recursos de formación gratuita, alertas tempranas sobre nuevas amenazas y guías específicas para pymes y ciudadanos, el INCIBE actúa como un puente entre la sofisticación técnica de la amenaza y la capacidad real de respuesta de la mayoría de actores del mercado.

Sus iniciativas de sensibilización —campañas sobre phishing estacional, alertas por categoría de industria, recursos adaptados a sectores con menor cultura digital— representan una de las pocas palancas de cambio sistémico disponibles a corto plazo. Pero el conocimiento de estos recursos sigue siendo insuficiente entre el público general y las pequeñas empresas.

✓ Qué hacer: Consulta el catálogo de recursos del INCIBE en incibe.es. Incluye guías gratuitas para empresas y ciudadanos, un teléfono de ayuda (017) disponible 24 horas, y alertas en tiempo real sobre amenazas activas.

Lo que tú puedes hacer hoy: de usuario a usuario con criterio

Ninguna medida estructural sustituye al criterio individual. Y el criterio se construye con información. Estas son las prácticas que marcan la diferencia real entre un usuario que el sistema puede proteger y uno que lo hará especialmente vulnerable:

Antes de introducir tu tarjeta en cualquier tienda

Verifica que la URL comienza por https:// y que el dominio es exactamente el correcto (no amazon-ofertas.com, sino amazon.es). Desconfía de precios que desafían la lógica. Busca reseñas del vendedor en plataformas independientes. Y si la tienda es nueva para ti, considera usar una tarjeta virtual de un solo uso, que muchos bancos ofrecen ya sin coste adicional.

Con los correos sobre pedidos y entregas

Es el vector de ataque más explotado del e-commerce. Antes de hacer clic en cualquier enlace de un correo que informa de un problema con tu pedido, entra directamente en la web de la tienda o el servicio de mensajería escribiendo la URL tú mismo. Nunca desde el enlace del correo. Esa fricción de diez segundos puede salvarte de un problema que tardará semanas en resolverse.

Con tus cuentas en plataformas de compra

Activa la verificación en dos pasos en cualquier plataforma donde tengas una tarjeta guardada. Usa contraseñas únicas —un gestor de contraseñas como Bitwarden (gratuito y de código abierto) resuelve esto sin esfuerzo. Y revisa periódicamente las compras y accesos recientes desde el historial de tu cuenta.

✓ Qué hacer: Activa alertas de transacción en tu banco para cualquier movimiento. Es la forma más rápida de detectar un fraude y actuar antes de que el daño sea mayor.

La reflexión estratégica que el sector necesita tener

Hay algo estructuralmente problemático en cómo la industria del e-commerce ha gestionado históricamente la seguridad: como un coste, no como una propuesta de valor. El HTTPS se implementó porque los navegadores empezaron a marcar las webs sin él como "no seguras". La autenticación reforzada llegó después de brechas masivas. La concienciación del usuario se ha dejado, en gran medida, a la iniciativa individual.

El resultado es un ecosistema donde el usuario lleva una parte desproporcionada de la responsabilidad de su propia protección, con herramientas y conocimientos insuficientes para el nivel de sofisticación de las amenazas a las que se enfrenta. Y eso no es sostenible en un mercado que quiere seguir creciendo sobre la base de la confianza.

Las empresas que van a liderar el e-commerce español en los próximos años no serán necesariamente las que tengan el mejor catálogo o los precios más competitivos. Serán las que consigan que sus clientes sientan que su información está genuinamente protegida, que hay consecuencias reales para quien falla en ese compromiso, y que la experiencia de compra segura no requiere que el usuario sea un experto en ciberseguridad.

La seguridad como ventaja competitiva es el próximo frente en el comercio digital español. Las empresas que lo entiendan antes tendrán una ventaja significativa. Las que lo sigan tratando como un trámite regulatorio lo aprenderán de la peor manera.

"La ciberseguridad ya no es un problema técnico. Es un problema de cultura. Y las culturas las construyen las personas, no los sistemas."