Cómo proteger tu negocio online

PorCarlos E Rivera
NOV 4, 2021

En 2018, la Condusef recibió 2 millones de reclamaciones por un posible fraude cibernético en tan solo 6 meses

El Buen Fin está a unos días de llevarse a cabo, del 10 al 16 de noviembre, el Cyber Monday se celebrará el 29 de noviembre y con esto inicia la temporada de compras de fin de año, por lo que Data Warden la empresa especializada en servicios de ciberseguridad recomienda tomar acciones preventivas al momento de realizar compras por Internet, debido al incremento de estafas online que puede hacerse presente durante época.

El confinamiento provocó que muchas personas optarán por adquirir sus productos y servicios a distancia, y además impulsó a muchas empresas a que cambiaran sus esquemas de venta y ahora lo hacen vía internet.

En el documental eLíderes de la Transformación Digital, realizado por el eCommerce Institute y la Asociación Mexicana de Venta Online (AMVO), en el cual se asegura que en México el ecommerce creció 81% en 2020 en comparación con 2019, adquiriendo un valor de 316,000 millones de pesos a causa del confinamiento por la pandemia.

Tan solo en 2018, la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef) recibió 2 millones de reclamaciones por un posible fraude cibernético en tan solo 6 meses. Y las cifras van en aumento cada año.

“Es por ello que las empresas deben protegerse de hackers y ataques que quieren robar datos de empleados y clientes para obtener dinero de las cuentas. A raíz de la pandemia muchas organizaciones han crecido en ventas online, pero sus niveles de seguridad digital son bajos, no les ha dado tiempo de protegerse adecuadamente”,

afirma Jesús Navarro, CEO de Data Warden. Hay varios niveles para proteger un negocio online. El primero de ellos es el básico y hay que realizar las siguientes acciones:

1. Elige una plataforma de comercio electrónico de una marca conocida y de buena reputación.
2. Utiliza los certificados SSL, que permite navegar con el protocolo https:// (la “s” significa seguridad), lo que da más confianza a los clientes. Estos certificados encriptan los datos, como nombres, contraseñas y números de tarjetas.
3. Ofrece varias formas de pago a tus clientes, no sólo con tarjetas de crédito o débito, también depósitos en tiendas de conveniencia o mediante aplicaciones universales, como PayPal.
4. Coloca varios pasos para la identificación de un cliente. Normalmente un ciberatacante cuenta con el número de tarjeta de la víctima, pero no cuenta con otros datos, como fecha de nacimiento, dirección física, NIP, correo electrónico o número de seguridad de la tarjeta.
5. Monitorea las direcciones IP de donde están llegando las solicitudes de compra; si hay muchas compras desde esa misma dirección, lo más seguro es que sea un fraude.

El siguiente nivel de seguridad que deben tomar en cuenta las empresas que venden online tiene que ver con la parte técnica y de consultoría:

1. Utiliza productos y asesoría de terceros, es decir, de expertos en ciberseguridad. Son las personas más adecuadas para proteger un sitio web.
2. Instala servicios avanzados de ciberseguridad, como el patrullaje en internet para detectar sitios falsos y páginas que se hacen pasar por la tienda original.

Actualmente, los hackers ya no están atacando al sitio directamente, sino que crean sitios falsos e incluso páginas en redes sociales para engañar a los clientes.
“Recomiendo realizar un servicio de patrullaje online, el cual no es un producto que se activa y listo, como un antivirus. Se trata de expertos que utilizan una docena de productos y ciberinteligencia para hacer una investigación de lo que hay en internet relacionado con la página web de la empresa y sus productos”, comenta Navarro.

Se buscan y analizan logos, palabras y letras similares, entre otros aspectos, para detectar si hay sitios o páginas en redes sociales similares o casi idénticas. Es como un espía rápido y eficiente que se cuela por todos los ámbitos de internet, incluyendo la deep web y la dark web, espacios donde se venden datos de usuarios, de tarjetas de crédito y hasta identidades de empleados de compañías.
Y un tercer nivel de protección se halla en la cultura de ciberseguridad de las empresas.

1. La seguridad de la información de la organización debe ser un pilar del negocio.
2. Se debe invertir en ciberseguridad; el presupuesto debe contemplar siempre este rubro.
3. Debe haber una capacitación constante de los empleados en ciberseguridad y también es necesario que las empresas eduquen a sus clientes dando continuamente recomendaciones sobre cómo proteger sus datos y su dinero.

Para conocer más sobre la soluciones de Data Warden consulta DataWarden.com

Acerca de Data Warden

Data Warden es una empresa mexicana líder en la implementación de soluciones integrales de ciberseguridad. Cuenta con un portafolio de servicios de clase mundial que abarca el ciclo de vida completo de los proyectos, desde su concepción con servicios de consultoría, su implementación con la integración de arquitectura tecnológica, hasta su operación con servicios administrados. Data Warden cuenta con las capacidades técnicas, corporativas y financieras necesarias para desempeñarse como el socio tecnológico de confianza de las empresas para poder llevar a cabo proyectos de alto impacto y valor en su organización. Mantiene un Sistema de Gestión Integral certificado bajo las normas ISO 9001:2015 e ISO 37001:2016, y cuenta con el Distintivo de Empresa Socialmente Responsable. Actualmente se encuentra en proceso de adopción y certificación de las normas ISO 20000 e ISO 27001. Para conocer más sobre Data Warden visita DataWarden.com