Lista de comprobación sobre ciberseguridad en el comercio electrónico internacional.

La ciberseguridad es un factor esencial a tener en cuenta en el comercio electrónico internacional. Esto se debe a que las transacciones internacionales de comercio electrónico a menudo implican la transferencia de datos sensibles, como datos financieros y personales, a través de las fronteras.

Para garantizar la seguridad de estos datos, las organizaciones deben emplear diversas medidas de seguridad, como el cifrado, las pasarelas de pago seguras y la autenticación de dos factores.

Además, las organizaciones también deben asegurarse de que sus sitios web cumplen las leyes internacionales de privacidad y seguridad de datos.

Las organizaciones deben vigilar sus redes en busca de actividades sospechosas y tomar las medidas adecuadas para protegerse contra las ciberamenazas.

Esta herramienta está diseñada para que los usuarios sepan si su empresa de comercio electrónico internacional cuenta con medidas básicas de protección contra ciberataques. Las grandes empresas suelen tener departamentos dedicados a estas funciones, pero las pequeñas suelen necesitar más recursos para ello.

Esta herramienta te dará una visión global de lo bien protegida que está tu empresa contra la ciberdelincuencia y tal vez identifiques lagunas o vulnerabilidades que se pueden abordar.

En cualquier caso, el usuario tomará conciencia de aspectos de la ciberseguridad que puede no haber tenido en cuenta y que está a tiempo de abordar, ya sea personalmente o a través de profesionales especializados.

Co-funded by the European Union

La herramienta es una lista de comprobación con preguntas relacionadas con la ciberseguridad y el comercio electrónico internacional. Para cada pregunta hay tres posibles respuestas en función de la experiencia del usuario:

SI: 

NO: 

NO LO SÉ: 

Supongamos que la mayoría de las respuestas son NO o NO LO SÉ. En ese caso, animamos al usuario a que se ponga manos a la obra para mejorar la seguridad de su negocio de comercio electrónico internacional y evitar así ser víctima de ataques que podrían acarrearle grandes pérdidas o incluso la quiebra del negocio.

Tras la lista de comprobación, los usuarios encontrarán una serie de consejos prácticos sobre ciberseguridad que les orientarán sobre los siguientes pasos a dar para mejorar la seguridad online de su empresa internacional.

Co-funded by the European Union

LISTA DE COMPROBACIÓN:

Preguntas			
¿Está tu sitio web de comercio electrónico debidamente cifrado para proteger la información de los clientes durante las transacciones?	☐	☐	☐
¿Has implantado políticas de contraseñas seguras para tus cuentas de cliente y administrativas?	☐	☐	☐
¿Actualizas regularmente el software de tu sitio web y los parches de seguridad para protegerte de vulnerabilidades conocidas?	☐	☐	☐
¿Dispones de un plan para responder a una posible violación de la seguridad, como un plan de respuesta a incidentes?	☐	☐	☐
¿Se tienen en cuenta todos los riesgos en la planificación empresarial? En caso negativo, ¿cuáles no?	☐	☐	☐
¿Has formado a tus empleados en las mejores prácticas de ciberseguridad, como por ejemplo cómo detectar y prevenir los ataques de phishing?	☐	☐	☐
¿Utilizas pasarelas de pago seguras y sigues los protocolos de seguridad estándar del sector para tratar y transmitir información confidencial de los clientes?	☐	☐	☐
¿Dispones de medidas para detectar e impedir el acceso no autorizado a tu sitio web y a los datos de tus clientes?	☐	☐	☐
¿Has realizado evaluaciones de seguridad y pruebas de penetración periódicas para identificar y abordar posibles vulnerabilidades en tu sistema de comercio electrónico?	☐	☐	☐
¿Dispones de políticas y procedimientos para eliminar de forma segura la información confidencial de los clientes cuando ya no se necesita?	☐	☐	☐
¿Dispones de un proceso de supervisión y revisión periódica de tus medidas de seguridad para garantizar que siguen siendo eficaces?	☐	☐	☐

Co-funded by the European Union

Consejos sobre ciberseguridad en el comercio electrónico internacional

1. Usa redes seguras: Asegúrate de utilizar redes seguras, como las redes privadas virtuales (VPN), para proteger tus datos mientras realizas transacciones de comercio electrónico.

2. Utiliza contraseñas seguras y únicas: Utiliza contraseñas fuertes y únicas para todas tus cuentas online y evita usar la misma contraseña para varias cuentas.

3. Activa la autenticación de dos factores: La autenticación de dos factores añade una capa extra de seguridad a tus cuentas online al requerir que introduzcas un código de un solo uso además de tu contraseña.

4. Mantén actualizados el software y los sistemas: Actualiza periódicamente el software y los sistemas para asegurarte de que dispones de los últimos parches y funciones de seguridad.

5. Utiliza métodos de pago seguros: Cuando realices transacciones de comercio electrónico, utiliza métodos de pago seguros, como pagos cifrados con tarjeta de crédito o sistemas de pago digital como PayPal

6. Ten cuidado con los ataques de phishing: Ten cuidado con los ataques de phishing, que son intentos de engañarte para que facilites información sensible, como tu contraseña o los datos de tu tarjeta de crédito.

7. Utiliza un software de seguridad de confianza: Utiliza un software de seguridad de confianza para proteger tus dispositivos y datos de malware y otras amenazas.

8. Ten cuidado al compartir información personal: Ten cuidado al compartir información personal, como tu nombre, dirección y datos de tu tarjeta de crédito, en Internet. Comparte esta información sólo con sitios web y comerciantes de confianza.

Co-funded by the European Union

9. Utiliza canales de comunicación seguros: Utiliza canales de comunicación seguros, como el correo electrónico cifrado o las apps de mensajería, para proteger tu información sensible mientras te comunicas con otras personas online.

10. Vigilar las posibles amenazas y violaciones de la seguridad y tomar medidas inmediatas en caso necesario

En general, la clave para una ciberseguridad eficaz en el comercio electrónico internacional es contar con una estrategia de seguridad integral que incluya una variedad de herramientas y tecnologías para protegerse contra las amenazas potenciales.

Gracias!

Co-funded by the European Union