Cómo reforzar la seguridad de tu tienda online: consejos y herramientas gratuitas

El comercio electrónico es una de las industrias que más rápido han crecido en estos últimos años. En 2020, la venta online en España creció un 36%, convirtiéndose en el tercer mercado que más ha aumentado de todo el mundo.

En un sector tan cambiante, y como dueño de tu tienda en línea, una de las cosas que debes tener en cuenta es la **seguridad**: tendrás que proteger tu negocio de posibles hackeos o, de lo contrario, podrías estar poniendo en riesgo tus datos y los de tus compradores.

¡Pero tranquilo! **Tomar las riendas de tus cuentas online y evitar ciberataques es más fácil de lo que parece.**

¿Estás preparado para garantizar la seguridad en tu tienda online? ¡Empezamos!

Qué es la seguridad online

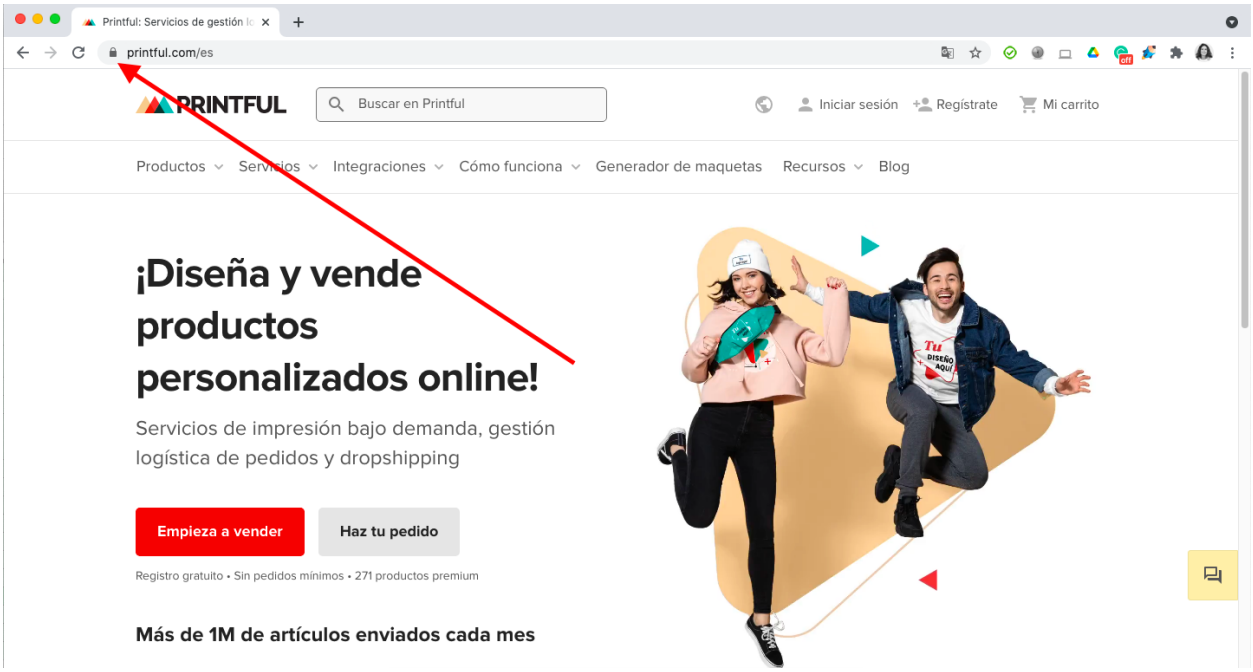
La seguridad online implica muchos factores: contar con un **buen antivirus**, tener certificados SSL para establecer una **conexión segura**, entrar en **sitios web fiables y seguros**, revisar tu correo electrónico y la privacidad de tus redes sociales, comprar en tiendas online de confianza...

Por ejemplo, Facebook sufrió un hackeo que afectó a más de 50 millones de cuentas. Un hecho así, aparte de que afecta al usuario, influye negativamente en la reputación de la empresa. Está claro que no podemos hacer nada frente a grandes brechas de seguridad como esta, pero **sí podemos estar preparados para saber qué hacer en caso de ataque**.

Y, aunque tu negocio online sea más pequeño, debes estar preparado para afrontar estos problemas.

Cómo puedes ser hackeado

La mayoría de los ecommerce cumplen con el **PCI-compliance** para mantener su seguridad online. Esto es un conjunto de **normas para proteger los datos de tu cliente cuando compra un producto en tu tienda online**. Si una página web cumple con esta medida, podrás ver un candado en la barra del navegador. Echa un vistazo a esta imagen de la página principal de Printful:



Si aplicas esto en tu tienda, los datos de compra de tus clientes estarán protegidos gracias a este estándar de seguridad.

Sin embargo, los hackers saben cómo atacar cualquier punto tecnológico por mínimo que sea, y tienen varias técnicas para hacerlo. Veamos cuáles son y cómo puedes protegerte frente a ellas:

Phishing

El phishing es un **sistema que los ciberdelincuentes utilizan para engañarte y conseguir datos personales** como contraseñas, tarjetas de crédito o número de cuenta bancaria. La mayoría de veces actúan a través de un correo electrónico falso o un mensaje de texto.

Lo que los ciberdelincuentes buscan con este método es **suplantar tu identidad**. Puede que alguna vez te haya llegado un correo electrónico sospechoso o un SMS en el que te piden información como tu dirección de email o datos personales.

No obstante, hay aplicaciones y extensiones especializadas, como **Netcraft para Chrome**, que te avisarán de posibles intentos de phishing en tu ordenador. Acuérdate de tenerlas actualizadas cuando te lleguen los avisos y lee bien el mensaje para no ir más rápido de la cuenta. Si no, cualquier hacker podría aprovechar tu descuido y hacerse con tus datos.

En el siguiente ejemplo, vemos un SMS que supuestamente indica la programación de la entrega de un pedido. Pero, en realidad, es una estafa. Durante el 2021, se ha alertado sobre SMS fraudulentos en nombre de compañías como SEUR, Amazon o Correos.

Ejemplo de SMS fraudulento suplantando a la compañía de transportes SEUR. (Fuente: SmileInformatica).

Otro de los factores que te puede ayudar a identificar estos **emails falsos es el genérico saludo "Querido/a", en lugar de tu nombre**. Si te fijas, las grandes compañías utilizan tu nombre para los emails importantes. ¡No te dejes engañar!

Cómo evitar el phishing:

Para que no se queden con tus datos, ya sea haciendo clic en un correo electrónico o con un SMS, pon en marcha estos consejos:

- Después de leer un correo electrónico con información difusa, no hagas clic en ningún enlace. **Accede directamente desde la URL del navegador a la página web**. Si lo haces desde el correo electrónico, ya estarás dando tus datos.
- **Actualiza siempre** el sistema operativo de tu ordenador y el de tu navegador web.
- Introduce tus **datos privados solo en sitios web seguros**. Para que un sitio se pueda considerar como 'seguro', mira si empieza por "https://" y que el navegador muestre el icono de un candado cerrado. ¡Es esencial fijarse en ese pequeño detalle!
- **No proporciones información confidencial a nadie** por teléfono ni por correo electrónico.
- **Aplica los parches de seguridad necesarios.**

Violación de datos

Cuando ocurre un ciberataque a una gran compañía, los datos de la mayoría de sus usuarios dejan de ser privados. Y si el hacker filtra la base de datos en internet, esta quedará visible para todo el mundo.

Si tienes una cuenta de correo electrónico que usas para casi todo y la compañía proveedora sufriera algún tipo de ataque, esta te avisaría para recomendarte cambiar tu contraseña. Y es importante que lo hagas: de lo contrario, puedes perder tu información privada.

Introduce tu email en la web de *haveibeenpwned.com* para asegurarte de que tus datos no han sido filtrados en algún ataque en el pasado. Esta herramienta te mostrará una larga lista de páginas web donde tus datos personales pueden haber sido violados (o no). En concreto te dirá tu nombre, tu correo electrónico y hasta tu posible contraseña.

Cómo mantener la seguridad en tu negocio online

Uno de los primeros pasos para mantener tu negocio online seguro es tener tu **software actualizado**. No vale con instalarlo y ya está: tendrás que estar atento a las continuas actualizaciones y encargarte de configurarlo. Si tienes cualquier problema, no dudes en acudir a un especialista para que te ayude.

Tener una buena seguridad en tu tienda virtual resulta crucial tanto para los datos de tus clientes como para los tuyos. De lo contrario, pueden salir a la luz informaciones confidenciales de tus usuarios, tus datos personales o incluso tus datos bancarios.

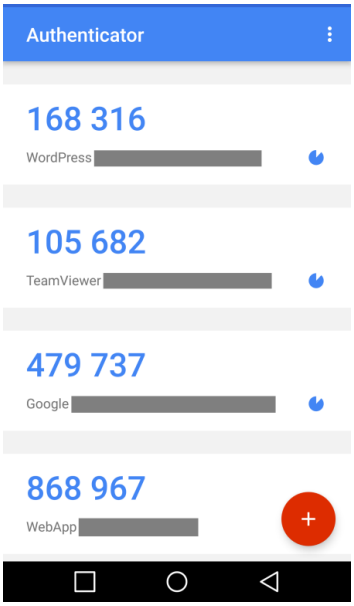
Si no quieres que algún hacker se quede con todas tus contraseñas guardadas en Google, configura la autenticación de dos factores.

Autenticación de dos factores (2FA)

Un estudio de Google desveló que **la 2FA previene el 96% de los ataques de phishing masivos**. Para activarla, tan solo tienes que asociar a tu cuenta Gmail a tu número de teléfono móvil para que, en caso de ataque, te llegue un código por SMS.

Hay aplicaciones como **Google Authenticator** o **Authy**, basadas en 2FA, que son muy simples de usar. Son apps gratuitas y compatibles con muchos sitios web, incluyendo Printful.

Los sitios que admiten 2FA deberían darte unos códigos de respaldo cuando te inscribas. Estos te servirán en caso de que pierdas tu móvil para acceder a la aplicación. ¡Guárdalos en un sitio seguro!



Fuente: Google Authenticator 2FA

Los mejores generadores de contraseñas

Si eres de los que solo tienes una o dos contraseñas para todo, te recomendamos que cambies ese mal hábito con un gestor de contraseñas.

Contar con un gestor de contraseñas te facilita el **uso de una contraseña única para cada una de tus cuentas**, lo que hace más difícil que los hackers usen datos de acceso filtrados en tu contra. También te ayudará a recordar tus contraseñas para no tener que cambiarlas a cada momento.

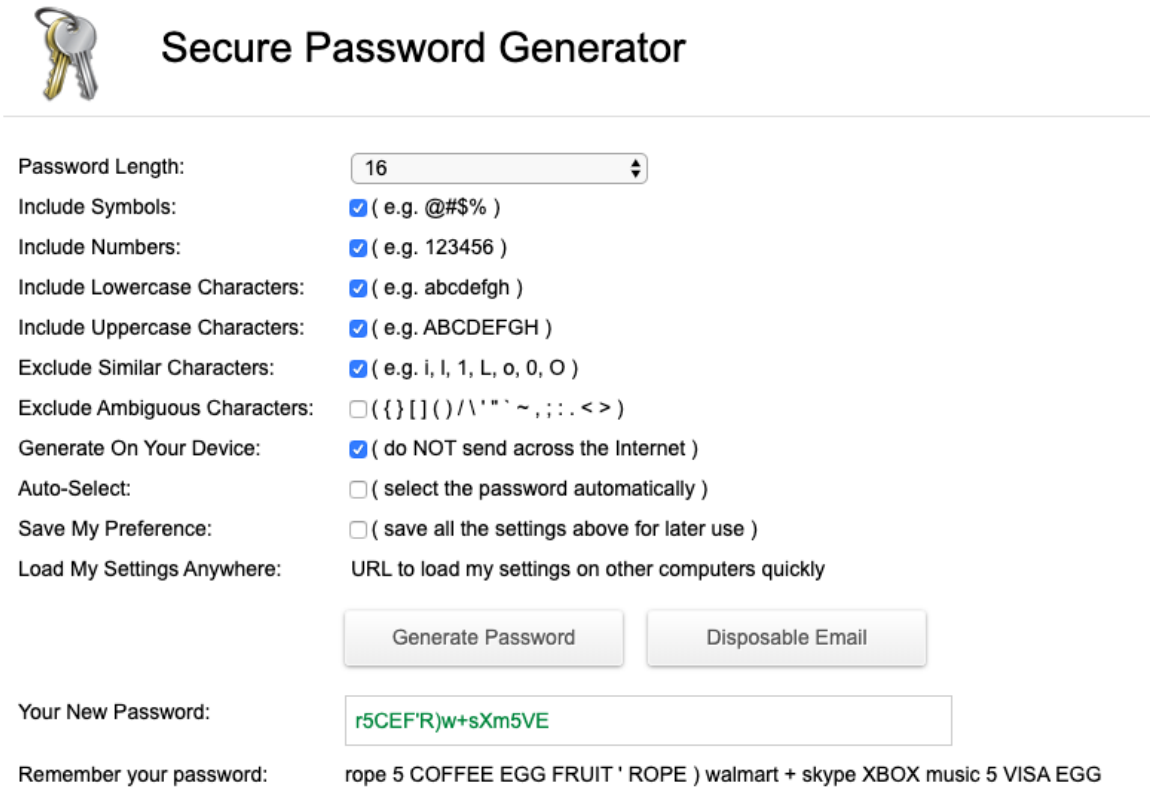
Lastpass

LastPass es uno de los mejores administradores y gestores de contraseñas. Una vez tus contraseñas estén guardadas, podrás iniciar sesión a golpe de clic de una manera rápida, sencilla y cómoda. Además genera contraseñas seguras, aleatorias o con números, lo que complica todavía más que un hacker las descubra y acceda a tus datos privados.

La aplicación es compatible tanto para Android como para iPhone. También cuenta con una extensión para el navegador web. ¡Lo tiene todo!

Password generator

Con la página web [Passwords generator](), o conocida en inglés como *Strong password generator*, podrás poner las preferencias que quieras a la hora de crear una contraseña. Puedes elegir si quieres incluir un número determinado de caracteres, mayúsculas o minúsculas, números o símbolos.



Fuente: [Secure password generator]()

Una vez hayas configurado cómo quieres que sea tu contraseña, esta aparecerá en *Your new password* y la podrás guardar en un sitio seguro. Para que no te olvides de la contraseña, la página la asocia con una palabra, una ciudad o incluso una fruta.

Bitwarden

[Bitwarden]() es la alternativa de código abierto ideal para organizaciones, empresas o tiendas online. Su función de uso compartido seguro permite compartir de forma segura las contraseñas cifradas con tus compañeros de trabajo. Resulta muy útil si tienes empleados, socios o proveedores que necesitan acceso a tus datos.

Puedes sincronizar los datos de tu tienda online con las personas que quieras sin que estos dejen de ser confidenciales. Lo mejor es que es compatible con todos los navegadores y plataformas.

Consejos para mejorar tu seguridad en internet

Para resumir, aplica estos 8 consejos para mejorar tu seguridad en internet:

1. Comprueba la seguridad de tu cuenta de Google. Tu cuenta de Gmail será por excelencia la que más utilices. Verifica tu cuenta de Google y descubre si estás al 100% de seguridad.
2. Revisa qué sitios web tienen acceso a tus datos personales. No tiene ningún sentido que tus datos personales estén almacenados en un sitio online que ya no utilizas, esperando a ser hackeados.
3. Asegúrate de que tus redes sociales tienen los ajustes de privacidad correctamente configurados. Por ejemplo, Facebook ofrece una herramienta de privacidad con la que puedes configurar la información que quieres que sea visible para tus amigos o para los amigos de tus amigos. Tampoco des datos comprometidos en tu perfil de Instagram.
4. Revisa si tienes alguna aplicación abandonada y que ya no utilices. Estas apps desactualizadas y en desuso son el blanco perfecto para los hackers. ¡No pongas tus datos en riesgo si lo puedes evitar borrando esas apps!
5. Échale un ojo a las respuesta que diste en las famosas preguntas de seguridad. No des datos simples que puedan ser fáciles de encontrar.
6. Evita conexiones públicas de redes Wi-Fi. Aunque suene muy tentador conectarse a una red Wi-Fi en la calle, es mejor no hacerlo.
7. Cierra tus sesiones en los ajustes preestablecidos. Si tienes muchas sesiones abiertas en diferentes páginas web, dales fin cerrando sesión.
8. No des tus datos personales o direcciones en bases de datos públicas.

Finalmente pregúntate, ¿te sientes ya seguro? Tu respuesta debería ser un sí rotundo tras aplicar estos consejos.

Toma el control de tu tienda online

Ahora que ya sabes cómo proteger tu tienda online, no te dejes atacar por ningún ciberdelincuente. Ve incorporando estas herramientas en tu día a día y aplica nuestros consejos para navegar por la red de forma segura.

¡Marca en la checklist siguiente todo lo que realices!

PRINTFUL

Checklist de seguridad para tu tienda online

- Comprueba la seguridad de tu **cuenta de Google**
- Revisa qué sitios web tienen **acceso a tus datos personales**
- Mantén tu **software** y tu **antivirus actualizados**
- Actualiza el **sistema operativo** de tu ordenador
- Da tus datos solo en **sitios web seguros:** mira si empieza por https://
- Crea una **contraseña única** para cada una de tus cuentas o tus redes sociales
- Configura tu **autenticación de dos factores**
- Evita conexiones públicas de **redes Wi-Fi**
- Cierra tus **sesiones en los ajustes preestablecidos**
- Asegúrate de que tus redes sociales tienen los **ajustes de privacidad correctamente configurados**