Cyber Monday: ¿grandes rebajas o grandes riesgos ciber?

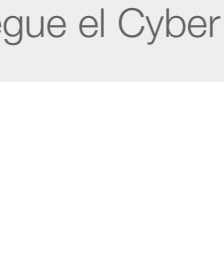
A todo el mundo le gustan las rebajas. El Cyber Monday está a punto de llegar y los consumidores van revisando sus listas de deseos, mientras los minoristas preparan sus sistemas para la **afluencia de compras.** Sin embargo, los ciberdelincuentes también planean su día de paga. El 34% de las empresas minoristas y mayoristas sufrieron un ciberataque en 2020[1]. Con miles de millones de euros en juego y unas ventas cada vez mayores, es importante **tomarse la ciberseguridad en serio.**

Ventas en el Cyber Monday[2]

2018	2019	2020
6.800 millones de Euros	**8.100** millones de Euros	**9.300** millones de Euros

€157.669 – el **coste medio de un ciberataque** para una empresa minorista o mayorista en 2020[3]. El riesgo es aún mayor si un negocio no puede funcionar durante una época tan ajetreada.

La ingeniería social, incluidos los ataques de phishing, causó el **39%** de los siniestros de Hiscox en 2020[4]. Este es un riesgo real tanto para las empresas como para los consumidores. Si una oferta parece demasiado buena para ser verdad, probablemente no lo sea.



Uno de los principales riesgos en torno al Cyber Monday, son los ataques de denegación de servicio distribuido (DDoS) que **aumentaron del 28%** en 2019[3] al **35%** para las empresas minoristas y mayoristas en 2020[3].

24% de las empresas minoristas y mayoristas **perdieron clientes y experimentaron mala publicidad** debido a un ciberataque[3].

Cómo pueden prepararse las empresas y los consumidores para el Cyber Monday

1 Mantén los sistemas actualizados

38% de las reclamaciones por interrupción del sistema fueron **causadas por vulnerabilidades del software**[5]. Asegúrate de que el software y las herramientas están configurados correctamente, se mantienen actualizados y se parchean contra cualquier vulnerabilidad. Como consumidor, asegúrate de que todos los dispositivos utilizados para comprar están actualizados.

2 Habilita la autenticación multi-factor (MFA)

Habilita la MFA en todas las cuentas de usuario, especialmente en las de administrador. Si un ataque de phishing tiene éxito, los niveles adicionales de seguridad para las cuentas mantienen **la información protegida**. Para los consumidores, opta por la MFA en todas las aplicaciones y cuentas cuando sea posible. Esto proporciona una **capa adicional de seguridad** para evitar que alguien entre en tus cuentas bancarias o de compras.

3 Prueba tu estrategia de copias de seguridad

Como empresa, **si se produce un ataque**, no querrás estar fuera de servicio durante mucho tiempo con el riesgo de perder ventas. **Asegúrate de tener copias de seguridad** realizadas con una frecuencia mayor y almacenadas offline. Prueba los escenarios de ataque antes de que llegue el Cyber Monday.

[1]Hiscox Cyber Readiness Report 2021
[2]Adobe digital insights
[3]Hiscox Cyber Readiness Report 2020
[4]Hiscox Annual Cyber Claims Report 2020
[5]Hiscox Cyber Claims Report Q2 2021

21828 11/21

HISCOX
CYBERCLEAR®