

Smishing o pharming: las nuevas técnicas de los ciberdelincuentes para robar este Black Friday

A las puertas de los grandes descuentos que llegan con el ya tradicional Black Friday, S2 Grupo destaca que el phishing, vishing, smishing, Social Media Phishing y el pharming, son las técnicas de suplantación de identidad que más van a utilizar los ciberdelincuentes en este periodo de ofertas. Expertos de la empresa de ciberseguridad han elaborado una guía de "buenas prácticas" para las compras online que "es esencial para hacerlo de una forma segura"

La empresa especializada en ciberseguridad y gestión de sistemas críticos S2 Grupo, ha advertido en un comunicado que debido a que se acercan fechas en las que se incrementan considerablemente las compras online y, por tanto, los ciberriesgos relacionados con el e-commerce es importante extremar las precauciones. Por esta razón, la compañía ha resaltado la importancia de conocer los ciberriesgos asociados al ecommerce con el fin de poder disfrutar de las compras de una forma segura.

“Si queremos protegernos de la ciberdelincuencia, necesitamos saber qué les motiva a actuar y cómo funcionan. Lo que buscan es dinero y datos personales, básicamente, porque precisamente esa información también vale mucho. Y en cuanto a su modo de actuación, hay que tener en cuenta que cada vez son más creativos y proceden a través de técnicas de ingeniería social”, ha explicado José Rosell, socio-director de S2 Grupo.

“Dentro de este tipo de técnicas, la más conocida es el phishing. Ésta consiste en que el ciberdelincuente suplanta una marca a través de un email, habitualmente, y ofrece una súper oferta que es el gancho para pinchar en el enlace que nos indican y al clicar, ya hemos caído en sus redes porque ese link es malicioso e instalara malware en nuestro dispositivo. Desconfiar de descuentos descomunales y no clicar en enlaces desconocidos es fundamental. Si dudamos, antes de acceder a través de ellos, es recomendable visitar directamente la web de la marca y buscar la oferta desde ahí”, ha enfatizado Miguel A. Juan, socio-director de S2 Grupo.

Junto al phishing, los expertos de la compañía de ciberseguridad han resaltado otras técnicas, cada vez más usadas como son:

El smishing: es un tipo de phishing que usa como canal el mensaje por SMS, por Whatsapp u otras aplicaciones de mensajería instantánea.

El vishing: esta usa la misma técnica pero a través de la llamada telefónica.

Social Media Phishing: cada vez es más común ver casos de suplantación de identidad en redes sociales.

Pharming: consiste en la creación de una página web maliciosa que ha creado el cibercriminal para que suplante la tienda online original y se dejen en ella los datos y dinero.

Buenas prácticas para las compras online

En cualquier caso, desde S2 Grupo se ha destacado que "conocer estos riesgos sólo debe servirnos para ser precavidos, ser conscientes de los posibles peligros y aplicar buenas prácticas del uso del ecommerce que nos permitan realizar las compras a través de este canal de una forma segura".

Según S2 Grupo, "las claves fundamentales de las cibercompras protegidas" son:

Acceder a la web de la tienda de forma manual. Poniendo directamente su dirección en el buscador.
Revisar los perfiles de sus redes sociales oficiales para confirmar que las ofertas están anunciadas y son reales. Si no aparecen, es aconsejable desconfiar rápidamente.
No comprar rápidamente por impulso y usar el sentido común.
Optar por formas de pago seguras.
Confirmar que la web comienza su dirección con el protocolo de seguridad "https".
Poner en duda cualquier mensaje que llegue con ofertas demasiado grandes.
Antes de comprar es aconsejable revisar las opiniones sobre esa web, las formas de pago, los datos fiscales, etc.
Usar conexiones a Internet privadas, no comprar desde wifis públicas y tener siempre activo un antivirus.

Datos de contacto:

Luis Núñez
667574131

Nota de prensa publicada en: [Madrid](#)

Categorías: [Finanzas](#) [E-Commerce](#) [Ciberseguridad](#)

NotasdePrensa

<https://www.notasdeprensa.es>