Las Últimas Noticias
29/11/2024 Audiencia: 271.020 Sección: ACTUALIDAD
$4.010.585 Tirada: 91.144 Frecuencia: DIARIO
$4.399.200 Difusión: 91.144
$4.399.200 Ocupación: 91,17%

Investigación de la Multinacional Check Point Research

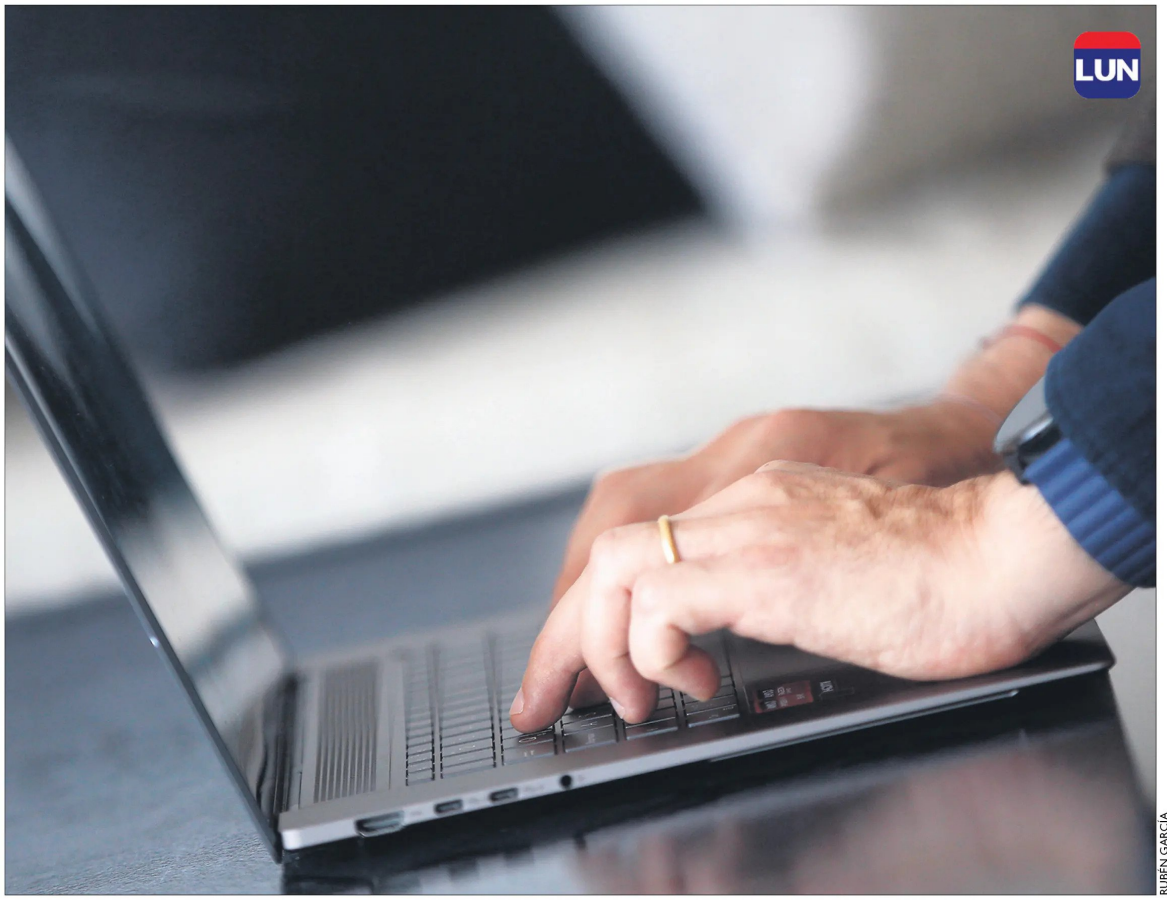
Creación de sitios web aumentó 89% por el Black Friday: cuidado con los que roban datos

Banyeliz Muñoz

El Black Friday es un evento digital que permite conseguir ese producto o viaje que tanto añoró a un súper buen precio. Si bien hay muy buenas oportunidades de compra, es importante tomar ciertas precauciones respecto a los sitios que visita. En principio, debe velar que sean marcas que estén asociadas al evento que promociona y organiza la Cámara de Comercio de Santiago (Cyber.cl https://acortar.link/kNhhwf).

Desde Vedata, una empresa que ayuda a las compañías a adoptar diferentes tecnologías, han detectado una serie de vicios que se dan durante esta temporada de compras. Entre ellas, que empresas ficticias envíen correos falsos a potenciales víctimas. "Es muy común recibir correos falsos durante el Black Friday. Los ciberdelincuentes aprovechan el aumento de las compras en línea para enviar correos electrónicos fraudulentos que parecen ser de tiendas legítimas. Estos correos buscan robar información personal o financiera", alerta Fernando Abrego, cofundador de esta firma.

Especialista entrega algunas claves para evitar ser estafado durante este evento digital: si le llega un correo que dice "urgente", por ejemplo, sospeche.



RUBÉN GARCÍA

No se deje llevar por la euforia al encontrar una oferta. Compruebe primero si es real.

¿Cómo se puede detectar?

"Lo más importante es verificar el remitente. A menudo las direcciones de correo electrónico falsas contienen errores en el dominio o parecen sospechosas. También cuentan con errores gramaticales o de redacción. Muchos incorporar enlaces y botones sospechosos. Por eso es recomendable que no haga click en enlaces ni descargue archivos adjuntos de correos no solicitados".

Ahora bien, si el correo dice "urgente", debe tener mayor precaución. "Si el correo menciona una acción inmediata o algo urgente, es una señal de alerta. Las tiendas legítimas no suelen presionar a los clientes de esa manera", explica.

Otra estafa común que observa es que hay muchos sitios web de tiendas que son falsos. De hecho, la compañía Check Point Research, especializada en amenazas cibernéticas, descubrió que la cantidad de nuevos sitios web creados en las dos semanas previas al Black Friday ha aumentado un 89% en comparación con 2023 y es más de tres veces mayor que en 2022. La mayoría de ellas son destinadas a robar la información personal y de pago de los consumidores.

"Las tiendas falsas pueden ser muy convincentes, por eso es importante saber verificarlas. Una de ellas es comprobar su URL. Debe asegurarse de que la dirección web (URL) esté correctamente escrita y sea segura. Las tiendas auténticas usan URLs que comienzan con "https://" y no con "http://", ejemplifica.

También llama a revisar las opiniones y reseñas. "Las tiendas legítimas tienen reseñas verificadas y están bien establecidas en sitios de confianza. Además, también suelen ofrecer formas claras de contacto (teléfonos, correos electrónicos y direcciones físicas)".

A su vez, aconseja buscar señales de confianza en el sitio. "Ideal que cuente con el logotipo de seguridad (candado) en el navegador al hacer compras o utilizar métodos de pago conocidos como PayPal o tarjetas de crédito", precisa.

Ofertas reales

El especialista sostiene que las ofertas de Black Friday a menudo usan tácticas de marketing sicológico para crear un sentido de urgencia. Sin embargo, dice que hay formas de distinguir entre una oferta real y una engañosa. "Lo más importante es investigar el precio real. Debe verificar el precio original del producto antes del descuento. Las ofertas reales son significativas, pero no deben ser excesivas".

"También es clave comparar los precios en diferentes sitios. Se aconseja usar comparadores de precios en línea para asegurarse de que la oferta es competitiva. Si algo parece demasiado bueno para ser cierto, probablemente no lo sea. Descuentos del 90% o más a menudo son una señal de alarma", advierte.

Abrego llama a realizar compras desde conexiones seguras, sobre todo para proteger su información personal y financiera. "Las conexiones seguras (HTTPS) cifran la información, lo que hace mucho más difícil que los ciberdelincuentes intercepten y roben tus datos. Si la conexión no es segura, podrías estar visitando un sitio web falso o comprometido que está diseñado para robar su información", comenta.

Recomienda evitar conectarse a wifi públicas, dado que pueden vulnerar su privacidad y puede dejar expuesto sus datos personales. "Trate de utilizar una wifi de un lugar muy serio y reconocido. O más seguro aún, compartir la wifi de su celular y utilizarla para una navegación segura".