Noticias

Black Friday y ciberseguridad

Escrito por: Horiens - 06/11/2023

Black Friday | ¿Usted sabe hacer compras online de forma segura?

Vea una guía rápida para no caer en estafas digitales, tornarse víctima de robo de datos y perjuicio. Información y concientización son pasos fundamentales para reducir riesgos.

El Black Friday, fecha conocida por la liquidación total en el mercado minorista, suele traer buenas oportunidades de compras no solamente en la fecha oficial, que en el 2023 será el día 24/11, sino a lo largo de todo el mes de noviembre.

¡Es importante tener atención, no obstante, a la hora de las compras! Si por un lado los descuentos proliferan, por otro lado aumentan también los riesgos de comprar online. Especialistas en seguridad digital indican que el Black Friday 2023 será campeón en ataques cibernéticos.

Los riesgos cibernéticos están entre los principales riesgos de la actualidad, afectando tanto a personas físicas como a empresas. “Muchas veces, incluso, ataques contra empresas comienzan fuera de ellas, por medio de los colaboradores en sus rutinas personales en Internet”, explica Ronaldo Andrade, CISO (Chief Information Security Officer) en Horiens.

“Horiens apoya a las empresas a tratar con riesgos, entre ellos los riesgos cibernéticos. La divulgación de informaciones preventivas y la concientización de colaboradores es parte esencial de una cultura de prevención y seguridad de la información”, completa.

Compartimos a continuación 10 consejos de ciberseguridad que valen no solamente para este período, sino siempre que usted haga cualquier compra por e-commerce.

Verifique la dirección del sitio web con atención para comprobar si no hay letras cambiadas y observe si el URL está precedido de un candado y de la sigla “https”.

No use redes públicas para hacer compras online, haga esto siempre desde su red particular.

Verifique la reputación de la tienda en sitios web como “Reclame AQUÍ”, “gov.br” y “Procon-SP”.

1. No salve informaciones de la tarjeta en el navegador ni en el sitio web del e-commerce.
2. Nunca informe la contraseña de la tarjeta de crédito o débito en la transacción de compra.
3. Verifique el valor de la compra y del flete dentro del carrito virtual, antes de hacer el pago.
4. Use la tarjeta en sitios web de empresas conocidas, en las cuales esté acostumbrado a comprar. Como alternativa, en otros sitios web utilice la opción de pago por PIX o boleto.

5. Al usar tarjeta, prefiera la versión “tarjeta virtual”, que es habilitada para compras por período determinado, reduciendo el riesgo de clonación.
6. Para hacer pagos con más seguridad por medio de apps de celular, habilite la configuración de autenticación de identidad por biometría, siempre haciendo uso de un segundo factor de autenticación.
7. Antes de pagar boletos, analice si él es verdadero de hecho, verificando informaciones de la operadora de crédito, banco o sus propios datos personales. Verifique también si el establecimiento receptor es el mismo para el cual usted realizó la compra.

En el caso que sea víctima de cualquier estafa, abra un Reporte Policial en la comisaría de crímenes virtuales. Cada estado tiene su respectiva comisaría. Vea a continuación el acceso a las de São Paulo, Río de Janeiro y Bahía.

SP: https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/pages/comunicar-ocorrencia/outras-ocorrencias/local-e-hora-da-ocorrencia

RJ: https://dedic.pcivil.rj.gov.br/

Bahía: https://www.delegaciadigital.ssp.ba.gov.br/OcorrenciaInternet/Bemvindo.ssp