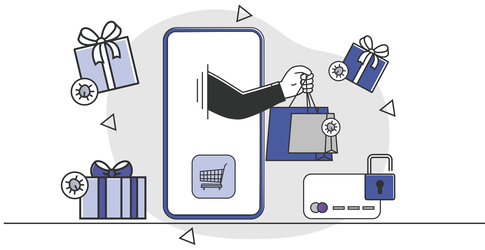
LOS CIBERATAQUES MÁS COMUNES EN BLACK FRIDAY Y CYBER MONDAY

Llega el Black Friday, las ofertas en los productos más atractivos y por ende las ganas de compra. Hoy, 25 de noviembre, se celebra en el **Black Friday**, y el lunes 28 el **Cyber Monday. Unas fechas señaladas en las que los cibercriminales son más activos debido al gran número de compras online.**

Con el auge de este periodo **se inaugura la temporada de compras navideñas con significativas rebajas en muchas tiendas** y de tradición americana cada vez más arraigada en Europa, **muchos son los usuarios que aprovechan para para encontrar los mejores precios para sus regalos**. **Uno de los fines más comunes de los hackers o piratas informáticos es la estafa.**



¿SABES CUÁLES SON LAS CONSECUENCIAS QUE PUEDES SUFRIR EN CASO DE NO TENER TODOS LOS SENTIDOS ACTIVADOS?

Phishing: Hace referencia al envío generalizado e indiscriminado de correos electrónicos a una lista de direcciones, sin un destinatario concreto. Ejemplo de ello puede ser una campaña en la que ofertan el último modelo de smartphone a precios extremadamente bajos.

Typosquatting: Es una forma de ciberataque en el que explota los fallos que cometemos a la hora de escribir direcciones web en la barra de nuestro navegador. De esta forma, acabamos visitando, sin querer, páginas alternativas que normalmente tienen propósitos fraudulentos.

Spam: Suele definirse como el correo electrónico no solicitado enviado de forma masiva, pero el término es mucho más amplio. Spam es cualquier mensaje inapropiado, molesto y no deseado que se envía a un gran número de usuarios, ya sea por correo electrónico, WhatsApp, SMS, redes sociales o incluso llamando por teléfono.

Adware: Es un tipo de software cuyo objetivo es forzar al usuario a ver publicidad en un dispositivo de manera no deseada e incontrolada. Para conseguirlo puede lanzar anuncios de manera aleatoria, redirigiendo búsquedas a webs de publicidad a las que no iríamos de ser por el adware.

Chargeback o devolución forzosa: Ocurre cuando tu banco o proveedor de pago te sustrae un cobro recibido, generalmente como consecuencia de haber aceptado una tarjeta fraudulenta.

E-skimming: es la versión digital del skimming de tarjetas de crédito. Mientras que en el mundo físico, los skimmers se instalan sobre los lectores de tarjetas de crédito para leer la información de la tarjeta de crédito, los e-skimmers son fragmentos de código malicioso que roban los datos de la tarjeta de crédito de un cliente durante una transacción en línea.

Robo de datos personales, bancarios, claves… Cuando caemos en las trampas que nos ponen en el camino los ciberdelincuentes podemos acabar proporcionándoles de una forma voluntaria e ingenua nuestros datos personales, llegando así a ofrecerles nuestros datos bancarios.

SI NO QUIERES CAER EN EL JUEGO DE LOS CIBERATACANTES, ACTIVA TODOS TUS SENTIDOS, PIENSA ANTES DE HACER CLIC Y SIGUE ESTOS CONSEJOS:

1.Comprueba tu conexión: Protégete al usar WiFi públicas mediante una VPN.

2.Comprueba que la URL de la tienda en la que te encuentras es la correcta. Muchas veces solo nos fijamos en la apariencia de la web y en el candado. Emitir un certificado para una web es bastante sencillo y de poco coste por lo que es importante también verificar la URL.

3.Confirma si la tienda online es fiable. Realiza compras solo en e-commerce confiables, conocidas o que cuentan con políticas de privacidad y condiciones de compra seguras.

4.Cuidado con los precios especialmente bajos. Duda de ofertas muy vistosas o de rebajas más altas de lo habitual.

5.No uses tu tarjeta de crédito. Puedes usar tarjetas virtuales.

6.Protege tu cuenta bancaria. No guardes el número de cuenta bancaria en ninguna página web.

7.Usa contraseñas robustas o cámbialas con frecuencia.

8.Mantén actualizados tus dispositivos. Asegúrate de que estén libres de malware e infecciones y haz uso de un sistema antivirus.

Si has detectado algún intento de fraude o ciberataque, avísanos para que nuestro equipo técnico especializado de respuesta a incidentes, toma las medidas oportunas para evitar su propagación y alerta a la comunidad sobre el riesgo.

SI IDENTIFICAS UNA CAMPAÑA ACTIVA DE MALWARE O PHISHING PUEDES AVISARNOS:

Llamando al 900 104 891

Enviando un email a incidencias@bcsc.eus

cyber zaintza