GUÍA PRÁCTICADE CIBERSEGURIDAD

... PARA REALIZAR COMPRAS ONLINE SEGURAS

En fechas tan señaladas como *Single Day*, *Black Friday*, *Cyber Monday* o *la campaña de navidad*, los ciberdelincuentes aprovechan y envían correos ***phishing masivos*** que enlazan a sitios falsos, imitando a tiendas para obtener datos personales.

"Amazon, víctima de las redes del 'phishing' durante el Black Friday" Fuente: Crónica Global. 30/11/2019.
"El aumento del 'phishing' amenaza el Día del Soltero y el Black Friday: hasta 803.000 intentos de ataques en un día" Fuente: Europa Press. 11/11/2020.
"Aumenta el Phishing al comprar online por el Black Friday y navidad" Fuente: Redes Zone. 26/11/2019.

PROCEDIMIENTO

CONSEJOS

1. Piensa antes de hacer clic
Ten cuidado con los anuncios que animan hacer clic en los enlaces. No hagas clic, ve directamente al sitio web para verificar que la oferta sea legítima.

2. Protégete al usar WiFi públicas
Aunque la web sea segura, te expones a la acción de terceros.

3. Comprueba la barra de direcciones
Asegúrate de que estás en la web de la página oficial donde quieres comprar.

4. Echa un vistazo si la dirección web del eCommerce es segura
La URL debe comenzar con "https://" o "shttp://".

5. Comprueba si tienes un certificado válido
Los certificados SSL (Secure Sockets Layer) autentifican la identidad de un sitio web.

6. Verifica la información sobre la existencia del dominio
Si el dominio es muy reciente y está registrado a nombre de una entidad misteriosa, tus sospechas estarán justificadas.

7. Confirma si la tienda online es fiable
Antes de comprar busca opiniones online para detectar su fiabilidad. Si es una tienda fiable dará información de contacto, dirección física, etc.

8. Revisa la política de devoluciones
Atento a la letra pequeña.

9. Comprar online sin usar tu tarjeta de crédito
Usa tarjetas virtuales, paypal u otra cartera virtual.

10. Ten precaución con tu cuenta bancaria
Revisa los movimientos por si detectas actividad sospechosa.

11. Instala un gestor de contraseñas
Crea contraseñas aleatorias y robustas para cada eCommerce y utiliza la autenticación multifactorial siempre que sea posible.

12. Mantén actualizados tus dispositivos
Asegúrate de que estén libres de malware e infecciones y utiliza un antivirus.

Ayuda a mitigar las amenazas...

avisándonos de los fraudes que indetifiques llamando al 900 104 891 o enviando un email a incidencias@bcsc.eus. Tomaremos las medidas oportunas.

EUSKO JAURLARITZA GOBIERNO VASCO
cyber zaintza