RED AZUL INFORMA: **NOVIEMBRE – 2019**

LA POLICÍA NACIONAL RECUERDA UNAS PAUTAS PARA EVITAR FRAUDES Y ESTAFAS DURANTE LAS TRANSACCIONES *ONLINE* EN EL *BLACK FRIDAY*

La Policía Nacional recuerda que la mejor manera para evitar ser víctima de fraudes y estafas cibernéticas durante los días de *Black Friday* es hacer uso del sentido común y mostrar especial atención a las **premisas claves** que permitirán realizar compras seguras en la red.

Los expertos en fraudes y estafas cibernéticas de la **Unidad Central de Ciberdelincuencia de la Policía Nacional** avisan de que los ciberdelincuentes aprovechan estos eventos, en los que se incrementan las compras y transferencias virtuales, para intentar engañar a sus víctimas potenciales.

Para evitar los cargos fraudulentos, la suplantación de identidad, la reconducción a una página web falsa o la remisión masiva de mensajes con ofertas irreales, entre otras muchas estafas, los especialistas proponen estas pautas que sirven como protección en cualquier tipo de transacción:

1. **No introduzca** su número de tarjeta en páginas web de dudosa confianza. Utilice siempre su sentido común y, en caso de duda, no realice la transacción.

2. **Asegúrese** de que sea un sitio seguro. Para ello, compruebe que aparece el icono de un candado en la barra de direcciones de su navegador.

3. **Verifique** regularmente que los cargos recibidos en su cuenta bancaria se corresponden con las compras que ha realizado.

4. **Utilice** plataformas intermedias de pago, con tarjetas prepago o con saldo reducido.

5. **Establezca**, siempre que sea posible, una doble comprobación para aprobar la transacción (un código del banco remitido a su móvil, tarjeta de coordenadas, etc.).

6. **Conserve** siempre el ticket o justificante de la transacción de cualquier tipo de compra para poder realizar las reclamaciones correspondientes en caso de productos defectuosos o que no respondan a lo esperado.

Las principales estrategias que han seguido los ciberestafadores durante los últimos años han sido diseñadas para conseguir su objetivo de engañar a los compradores durante sus transacciones. Entre ellas, la Policía Nacional destaca:

- El ***carding*** consiste en la utilización fraudulenta de numeraciones válidas de tarjetas de crédito para efectuar compras por Internet, es decir, los cargos fraudulentos contra una tarjeta de crédito, de la que han obtenido las credenciales a través de otros procedimientos o por ataques a bases de datos de clientes de entidades o empresas. Una vez obtenidas esas credenciales, el estafador controla completamente la tarjeta para operar con ella libremente hasta que su titular original proceda a su anulación.

En la mayoría de los casos las credenciales se obtienen también al realizar transferencias electrónicas fraudulentas, que consiste en engañar a las víctimas con ofertas comerciales tan atractivas como falsas con el fin de conseguir los datos y claves bancarios o de tarjetas de crédito, pagos o transferencias indebidos, etc. Una vez que la víctima ha realizado la trasferencia a una cuenta controlada por la organización, desaparece todo rastro de los vendedores y, por supuesto, también del producto ofertado.

- El ***phishing*** es otro método utilizado por los ciberdelincuentes para suplantar la identidad de una empresa y engañar a sus víctimas. A través de correos electrónicos, que contienen una página web duplicada con apariencia legal (de bancos, organismos, empresas, etc), la víctima, -confiada de estar ante una página oficial-, proporcionará los datos que le solicitan y que posteriormente utilizarán para cometer la estafa. Las entidades bancarias, empresas u organismos oficiales nunca piden información de claves por correo electrónico. En caso de sufrir uno de estos ataques, se aconseja comunicarlo a la entidad o banco suplantado.

- El ***pharming*** consiste en suplantar el nombre de dominio (DNS) de una web legal, para reconducir al usuario víctima, a una página web falsa. Una vez en ella, el procedimiento para robar sus datos será igual que el anterior.

- El ***spamming*** o remisión masiva de mensajes no solicitados con ofertas publicitarias de cualquier tipo, avisos falsos, cupones descuento u otros ganchos lo más atractivos y creíbles posible. Por eso, desde los perfiles en redes sociales de la Policía Nacional se reitera no abrir correos de usuarios desconocidos y eliminarlos directamente y nunca clicar en enlaces acortados de procedencia dudosa.

- El ***Vishing*** y el ***SMishing*** son variantes del *phishing*. En el caso del *Vishing* en los que el engaño se produce induciendo a la víctima a llamar a un número de atención al cliente falso. En el *SMishing* la trampa se realiza a través de *SMS´s.*

En el caso de sufrir alguna de estas modalidades delictivas póngalo en conocimiento de las Fuerzas y Cuerpos de Seguridad, mediante las vías de comunicación:

CIMACC 091 (Policía Nacional). Tratamiento de servicios de urgencia, a través del teléfono **091**.

RED AZUL (Policía Nacional). Tramitación de información a través del correo electrónico **redazul@policia.es.**