Prudencia y desconfianza para no ser víctima de *carding, phishing, pharmig, spamming* u otras estafas

La Policía Nacional recomienda cinco sencillas pautas seguras y mucho sentido común a la hora de comprar en el *Black Friday*

- **Vigila dónde y cómo usas tu tarjeta de crédito para evitar cargos fraudulentos, solicita la verificación en dos pasos con tu entidad bancaria y controla los cargos realizados con frecuencia**

- **A la hora de "clicar" en ofertas, comprueba que es la página oficial, no te dejes llevar por mails no solicitados u ofertas compartidas por WhatsApp y verifica siempre la URL del navegador**

- **Comprueba que estás realizando la compra desde un sitio seguro, -con un candado en la barra de direcciones-, y utiliza plataformas intermedias de pago o tarjetas específicas para compras *online*, prepago o con un saldo reducido**

23-noviembre-2017.- La Policía Nacional recuerda cinco sencillas pautas seguras, junto al sentido común, a la hora de realizar compras *online* durante estos días que proliferan las ofertas y webs con reclamos publicitarios vinculados al *Black Friday*. Los expertos en fraudes y estafas cibernéticas de la Unidad de Investigación Tecnológica de la Policía Nacional recuerdan 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 el *carding, phishing, pharming* u otra modalidad delictiva en las compras *online*, -además de la prudencia, sentido común y desconfianza racional-, los especialistas recuerdan estas cinco premisas que nos protegerán en nuestras transacciones:

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. Siempre que sea posible, establezca una doble comprobación para aprobar la transacción (un código del banco remitido a tu móvil, tarjeta de coordenadas, etc.)

En cualquier tipo de compra, se recomienda también conservar el ticket o justificante de la transacción para poder realizar las reclamaciones correspondientes en caso de productos defectuosos o que no respondan a lo esperado.

***Carding, phishing, pharming* y otros fraudes**

En los últimos años, ante el uso masivo de las tarjetas de crédito para realizar pagos y la normalización de las compras *online*, los ciberestafadores han ingeniado varias estrategias para engañarnos en nuestras transacciones.

- El *carding*, 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.*