CONSEJOS PARA LOS PAGOS VÍA PAYPAL Y BIZUM

Para más información
OFICINA MUNICIPAL DE INFORMACIÓN AL CONSUMIDOR
928 44 85 62
omic@laspalmasgc.es
www.laspalmasgc.es

Ayuntamiento de Las Palmas de Gran Canaria
TODA UNA CIUDAD
OMIC

Consejos para los pagos vía Paypal y Bizum

Ayuntamiento de Las Palmas de Gran Canaria
TODA UNA CIUDAD
OMIC

Consejos para los pagos vía Paypal y Bizum

Engaños más comunes con utilizar con PayPal:

1. Phishing: El phishing o suplantación de identidad es una forma razonablemente común de fraude en Internet, basada en el descuido de los usuarios en la Web. Para extraer datos personales, inicios de sesión, contraseñas, números de tarjetas bancarias u otra información vital de los usuarios, los estafadores crean páginas falsas de sitios de tiendas, bancos, clientes de correo electrónico y redes sociales. Visualmente, no se diferencian de los originales, por lo que un visitante desatento ingresa sus datos de autorización, luego de lo cual lo pierde todo.

2. Pago por adelantado: Es frecuente que sean el llamado fraude de pago por adelantado, una estafa clásica en Internet, para defraudar a los usuarios de PayPal. Las víctimas reciben una notificación de que se les debe una cierta cantidad de dinero, que podría ser debido a una herencia, la lotería o alguna otra compensación. Las opciones son ilimitadas, pero sea cual sea la historia, la víctima siempre tiene que hacer antes un pequeño anticipo (en este caso, a través de PayPal).

3. Inversiones y donaciones «benéficas»: En ocasiones, se hacen pasar por organizaciones benéficas para estafar el dinero de sus objetivos. Otra técnica de estafa de PayPal es ofrecer oportunidades de inversión muy baratas.

4. «Nombre descriptivo» o suplantación de nombre visible: Las estafas por correo electrónico de «nombre descriptivo» utilizan una función de los sistemas de correo electrónico que permiten ocultar el nombre del remitente detrás de un «nombre descriptivo» que puede parecer legítimo y engañar.

Consejos para utilizar PayPal:

1. Tener una contraseña segura: Tenemos que tener cuidado con que nuestra contraseña no sea demasiado sencilla. Evite fechas de nacimiento, teléfonos y otras sucesiones de números predecibles. Y por supuesto, no utilice la misma contraseña que la que utilice en otras aplicaciones bancarias.

2. Una cuenta de correo de usuario activa: Es importante que, al crear la cuenta de PayPal, elija una cuenta de correo que use de manera activa. Cada movimiento que se realiza desde PayPal va acompañado de una notificación vía e-mail. Así, si se hace alguna actividad con su cuenta sin su control, podrá consultar ese aviso y reaccionar de la manera más rápida posible.

3. Infórmese sobre el vendedor: La mayoría de sitios de compra online tienen un sistema para valorar los vendedores. No deje de consultar su puntuación, así como los comentarios que la gente deje al respecto de su funcionamiento. Si se trata de una tienda web, busque en foros alguna información sobre las experiencias de otros usuarios.

4. Consulte la política de devoluciones: Siempre que vaya a comprar, compruebe que haya una política de devoluciones, y si no la hay, contacte con el vendedor para confirmar.

Engaños más comunes con utilizar Bizum:

1. Solicitar dinero: Nos dicen que nos van a hacer el pago por Bizum, solicitándonos el número de teléfono para ello. Sin embargo, en vez de enviarnos el pago, lo que nos enviará será una solicitud de envío de dinero. El mensaje especifica que es una solicitud de dinero, pero si por las prisas o desconocimiento de cómo funciona Bizum, pulsamos en aceptar, estaremos enviando el dinero en vez de recibirlo.

2. Pedir pagos por adelantado: Aquí se ofrecen artículos en páginas de venta en internet por precios bastante atractivos o inferiores a lo normal. Una vez captado el interés de un comprador potencial, se pide que le adelante una parte del importe o el precio completo del producto para proceder a enviarlo. Sin embargo, una vez hecho el pago, la víctima no recibirá nunca el producto. Los estafadores que emplean este método se aprovechan de que no se puede anular un pago por Bizum (a diferencia de una transferencia bancaria normal), ya que el envío de dinero es instantáneo e irrevocable.

3. Supuestos abonos de la Seguridad Social: Se trata de un falso abono de la Seguridad Social por alguna prestación o por ERTE. En este caso, se envía un SMS a la víctima potencial o recurre a una llamada telefónica (vishing) en la que se hace pasar por la Seguridad Social y comunica a la víctima que le van a hacer un abono de una prestación pendiente. Dicho abono lo harán por Bizum, por lo que solicitan el número de teléfono y, como en el caso de solicitar dinero, lo que envían es una solicitud de envío de dinero. A veces, en el mensaje aparece el nombre «TGSS» para tratar de darle veracidad.

4. El aviso de pago por error a través de WhatsApp: Aquí, se le envía un mensaje de WhatsApp a la víctima, en el que se le comunica que por error le ha enviado un pago por Bizum de X cantidad de euros (lo más habitual son 50 €); aparentemente, quien envía el mensaje es alguien de la lista de contactos de la víctima. Si picamos, porque no nos paramos a comprobar que el supuesto ingreso es real, perderemos esos 50 euros.

Consejos para utilizar Bizum:

1. No compartir sus contraseñas: Nunca comparta las contraseñas o las credenciales de acceso de su banca digital. Si cree que alguien diferente a usted ha podido obtener de alguna manera estos datos, hay que cambiarlos de manera urgente.

2. No compartir información personal: Si recibe una llamada, un mensaje o un e-mail en el que le soliciten compartir datos personales como su nombre completo, número de teléfono, DNI, etc., nunca los facilite.

3. No aceptar solicitudes para recibir dinero: Tenga cuidado, en ocasiones se solicita dinero a particulares haciéndoles creer que deben aceptar ese pago para recibir la transferencia. Pero no es así. Lo que están confirmando es un envío y no la recepción. Para recibir dinero de otro contacto no necesita realizar ninguna gestión ni validación, simplemente verá el importe en su cuenta bancaria directamente o recibirá un SMS que confirme el movimiento.

4. Revisar bien las solicitudes de dinero: Si alguien le envía una solicitud de dinero por Bizum, compruebe que el importe y el nombre del destinatario sean correctos. Rechace la solicitud si no conoce quién le pide ese importe.

5. Usar Bizum en comercios web de confianza: No use Bizum al pagar en comercios que no cumplen con las normas de seguridad. Compruebe que la barra de dirección del navegador comienza con «https» y tiene el candado de seguridad. También, puede ver en la web de Bizum qué comercios están adheridos a la plataforma.