SUPLANTACIÓN O ROBO DE IDENTIDAD, CORREO, SERVICIO ONLINE Y REDES SOCIALES

RECOMENDACIONES PARA EVITAR TIMOS Y ESTAFAS Y MINIMIZAR LOS EFECTOS DEL PHISHING

- La mejor prevención es la información.

- No abrir la puerta a desconocidos y, si dispone de mirilla, comprobar siempre la identificación de las compras realizadas o reparaciones, por escrito.

- No pague servicios por adelantado. Compruebe antes el trabajo realizado.

- No guarde todo el dinero en su domicilio. No saque todo el dinero en efectivo de su pensión. Hágalo escalonadamente y procure ir acompañado o bien mire los días de cobro de la entidad bancaria para que lo haga por ventanilla, con seguridad.

- No lleve grandes cantidades de dinero en metálico, use tarjetas de crédito controladas.

- Camine siempre con el bolso por dentro, del lado de la pared.

- Desconfíe de los sorteos, rifas y regalos. No responda a las ofertas que no entienda sobre negocios que puedan enriquecerle rápidamente sin riesgos.

- No se fíe de los guías y pregunte siempre a su médico de familia o especialista.

- Destruya los recibos, comprobantes o extractos bancarios de las tarjetas de crédito y cuentas bancarias que no utilice.

- No revele información personal por teléfono si no está seguro de quien es el receptor. No hable sobre inversiones con personas que no sean de su confianza o entorno familiar.

- Procure no sacar cantidad de dinero en los cajeros automáticos. Sea prudente.

- Tape siempre el número secreto y no use uno demasiado fácil como es la fecha de nacimiento. Ello es fácil para los especialistas en este tipo de delitos.

- Nunca facilite el número secreto de su tarjeta a los empleados de Banco y no lo lleve por escrito en su monedero. Debe memorizarlo.

- Desconfíe de todos los técnicos que aparezcan sin previo aviso en su domicilio en nombre de alguna empresa. Compruebelo llamando a la misma (empresas de luz, gas, ...) Intente que haya algún familiar con usted para pedir opinión. No acepte que le convenzan.

- No ofrezca nunca datos bancarios y personales por la Red.

- Intentar siempre que el pago sea contra reembolso y no facilite datos bancarios. Acuda a métodos seguros de pago, como la transferencia bancaria que permite seguir el rastro del dinero.

- Huir de las compañías de envío de dinero como western Union, Money Gram ..., ya que son utilizadas frecuentemente por los delincuentes al no dejar rastro.

- Si se solicitan online pagos por adelantado, no hacerlo. Así mismo hay que huir de los precios desorbitadamente bajos con relación a los precios del Mercado ya que pueden esconder un fraude o estafa.

- De vital importancia descargar y guardar en lugar seguro todas las facturas y todos los pedidos en la empresa online elegida para futuras reclamaciones. Sirven para controlar los gastos y en caso de problemas tener justificantes.

- Desconfiar de anuncios en los que solicitan hacer uso de los teléfonos de tarificación adicional (803, 806, 807...).

Ayuntamiento de Las Palmas de Gran Canaria

TODA UNA CIUDAD

OMIC

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

www.laspalmasgc.es

SUPLANTACIÓN O ROBO DE IDENTIDAD EN EL CORREO, SERVICIOS ONLINE Y REDES SOCIALES

PASSWORD

SUPLANTACIÓN O ROBO DE IDENTIDAD EN EL CORREO, SERVICIOS ONLINE Y REDES SOCIALES.

El más frecuente es el de las redes sociales ya que la información se obtiene fácilmente e igualmente el hacerse un perfil igual al del usuario.

Cualquier persona puede ser suplantada y no es estrictamente necesario tener un perfil en internet donde aparezcan tus datos personales y no tengas controlados quien accede a los mismos.

Los delitos de suplantación de identidad tienen unas consecuencias legales y penales que dependiendo de los mismos y sus características, pueden llevar a penas de multas o prisión (art. 401 y 402 del Código Penal).

FORMAS DE SUPLANTACIÓN Y DELITOS MAS FRECUENTES:

Accediendo a la cuenta del usuario. El ciber-delincuente se hace con claves de acceso de la cuenta de la víctima activándolas o utilizando el PHISHING (una persona se hace pasar por una empresa conocida, Banca, Correos, Agencia Tributaria... Para que el usuario pague. Suplantación de identidad de una empresa o entidad pública de forma que la víctima crea que es un Organismo Oficial cuando no lo es).

Creación de un perfil falso utilizando información personal de la persona suplantada (fotos), vulnerando el art. 18 de la Constitución Española - Derechos de la propia imagen.

Revelación de secretos o lesión de privacidad (art. 197 del Código Penal), una persona se mete en el perfil de otra persona habiendo robado contraseñas o cuentas que le dan acceso al mismo. (Pueden penarse con prisión de 1 a 4 años y multa de 12 a 24 meses).

Ligado al anterior y recogido en el art. 264 del C. Penal, definir un sistema informativo para conseguir las contraseñas de una persona (penas de 6 meses a 2 años de prisión).

Implantar identidad con la fabricación de tarjetas de Crédito y utilizarlas en compras fraudulentas. Delito de fraude y estafa (6 meses a 3 años de prisión).

EL MAS IMPORTANTE DE LOS DELITOS HOY ES EL PHISHING.

Como evitar la suplantación:

Usar contraseñas robustas para acceder al perfil de la red social.

- Saber en que consiste el **Phishing** (método fraudulento en el que se suplanta la identidad de páginas webs conocidas u oficiales), o el **carding** (utilización en fraude de las numeraciones de tarjetas de crédito o débito válidas para realizar transacciones comerciales en tiendas online).

- Configurar los perfiles lo mas privados posible y así se evita que usuarios desconocidos accedan a nuestra información personal.

- Añadir usuarios y asegurar que sean conocidos. No es recomendable hacer amigos a todos los que solicitan amistad.

- No compartir fotos o videos comprometedores. Los ciber-delincuentes buscan este tipo de contenidos, para extorsionar a sus víctimas con la excusa de que si no lo hacer, harán público el video.

- Revisar la política de privacidad y las condiciones del servicio al que se está accediendo. Así conocerás el uso que hace la red social de tus datos, como los tratarán, almacenarán, como son compartidos, etc.

- Usar un antivirus actualizado e instalar y usar una solución antispyware.

- Activar el firewall de nuestro sistema operativo.

- Actualizar los programas como el sistema operativo de forma periódica.

- Ser precavidos a la hora de utilizar una conexión wifi pública y no introducir ningún dato sensible haciendo uso de ella.

- Tener cuidado con los archivos que descargamos y recibimos por correo.

- Eliminar cualquier correo que sea sospechoso o del que no se tenga constancia del origen, sin abrirlo.

- Borrar correos, spam o basura (no abrir sus adjuntos, ni acceder a sus enlaces).

- Evitar la cadena de mensajes, ya que son fuente de correos basura (spam), y un modo de recopilaciones de direcciones de correos electrónicos, fuentes potenciales de phishing. Para ello lo mejor es enviar los correos con destinatarios ocultos.

Hay que recordar que un Banco nunca va a solicitarte información del usuario, claves y datos personales a través de un correo electrónico.

Antes de introducir datos en una página web hay que asegurarse que se trata de un servidor seguro (la dirección de la página tiene que empezar por https, presencia de un candado en la barra de direcciones).

HACER COMPRAS POR INTERNET ES SEGURO SI SE SIGUEN UNA SERIE DE CONSEJOS O UNAS MINIMAS NORMAS SEGURAS:

- Escoger tiendas de confianza, para lo que es recomendable revisar la información de la página en cuestiones referidas a avisos legales, política de privacidad o términos de uso (normalmente esta información se encuentra en la base de la página a modo de enlaces). Las tiendas que operan en internet tienen certificado de seguridad.

- Para evitar fraudes y estafas hay que mirar y revisar la información de páginas.

- Si la tienda no se identifica correctamente online, se aconseja no comprar en las mismas.

- La empresa que ofrece sus servicios en línea deberá proporcionar: nombre completo de la misma (NIF, NIE, CIF), datos de inscripción en el Registro Mercantil, dirección postal y dirección de correo electrónico).

- No es recomendable realizar transacciones online si la empresa que vende o utilizas sus servicios a través de internet no se identifica convenientemente.

- Asegurarse que en el momento de aportar los datos para la transacción solo serán utilizados para la gestión de contratación, igualmente la tienda online debe informar de la posibilidad de ejercer los derechos reconocidos en la normativa vigente de protección de datos personales.

- Los menores de 14 años no podrán ofrecer su consentimiento para que sus datos personales sean tratados por la tienda online (tienen que hacerlo sus representantes legales).

- El comercio online debe informar de la utilización de cookies y permitir su aceptación o no.

- Las tiendas online deben poseer un certificado de seguridad (el navegador mostrará un icono con la forma de candado y la url empezará por https en lugar de http.

- El certificado de digital de la empresa (se obtiene pulsando el candado anterior), tiene que ser válido. Se desaconseja seguir con la operación si no es así.

- Es buena señal que la página cuente con la distinción en forma de sellos de confianza, como ejemplo, Confianza online.

- A la hora de realizar transacción a través de página web de la empresa, se solicitará a la parte compradora los oportunos datos personales que solo pueden ser utilizados para fines relacionados con la gestión de la contratación que se haga.

- Desde Consumo se insta a no aceptar nunca como método de pago, servicios de envío y recepción de dinero en efectivo, y en cuentas bancarias.

SI EXISTE SUPLANTACIÓN DE IDENTIDAD:

- Hacerse con pruebas, si es en internet, hacer pantallazos del perfil falso.

- Denunciar o querellarse para lo que hay que acudir a un abogado.

- Existen enlaces donde se explica donde y como denunciar la suplantación de identidad en las redes sociales(Facebook, Twitter, Istagram, Google...)

- Acudir a las Fuerzas de Seguridad del Estado (Guardia Civil, Policía Nacional), con PRUEBAS de la suplantación para que tenga validez total la denuncia.

Es importante acceder a la información y recomendaciones de la Guardia Civil para prevenir estos delitos de suplantación y estafas reguladas en el Código Penal art. 248.

Estafas + de 400€, cuantía de lo defraudado.

Delito leve de estafa cuando la cantidad no supere los 400€ (art. 249 del Código Penal).

Se ofrece una información exhaustiva de los perfiles de los estafadores, tipos de estafas más frecuentes, recomendaciones ante timos y estafas.

http:**www.guardiacivil.es/es/servicios/consejos/estafa.html**

/index.html http://www.policia.es/consejos/internet.html