Publicado en el 28/12/2013

En el Día de los Inocentes la Policía Nacional alerta de los nuevos fraudes y bulos que se propagan en las redes sociales

Im?genes

Smartphones, tablets y otros gadgets son las nuevas herramientas para jugarte una mala inocentada

En el Día de los Inocentes la Policía Nacional alerta de los nuevos fraudes y bulos que se propagan en las redes sociales

Phishing, suscripciones a SMS Premium, secuestros virtuales, "mulas" blanqueadoras, falsas ofertas de trabajo o venta de supuestos chollos que nunca llegan son algunos de los ciberdelitos que utilizan técnicas de ingeniera social para engañar a sus víctimas

Además, las redes sociales y aplicaciones como el Whatsapp se han convertido también en canales para viralizar bulos sobre supuestos secuestros de niños, calcomanías con LSD impregnado, colonias que te duermen o teléfonos-bomba dejados por terroristas

Mantener los equipos actualizados y protegidos; el sentido común y la desconfianza racional; utilizar plataformas seguras para las transacciones económicas; disponer de una tarjeta para pagos electrónicos y seguir las indicaciones de la Policía son algunos de los consejos para evitar ser víctimas de fraudes, estafas o timos

28-diciembre-2013.- La Policía Nacional alerta de los nuevos fraudes, estafas, timos y bulos que se propagan, con especial rapidez, en las redes sociales y aplicaciones de comunicación, como el Whatsapp, y cuyo objetivo es lograr un beneficio económico para los ciberdelincuentes o crear una alarma infundada entre la población. Con motivo del Día de los Inocentes, los especialistas de la Policía Nacional en seguridad tecnológica repasan los fraudes, falsedades o engaños más habituales detectados durante este año, desde los ya clásicos delitos de phishing o suscripciones mediante artimañas a servicios de SMS premium, a los nuevos secuestros virtuales o "mulas" blanqueadoras de dinero. Además, se reitera la existencia de bulos o ciberleyendas que se propagan y viralizan por las redes sociales y grupos de mensajería instantánea, como el secuestro de niños, calcomonías impregnadas de LSD, alertas de bombas en medios de transporte o centros comerciales, "robo" de órganos, colonias que adormecen o teléfonos-bomba abandonados por terroristas. Para evitar ser víctima de fraudes, engaños o timos, los agentes aconsejan mantener los equipos actualizados y protegidos; no olvidar el sentido común y la desconfianza racional; utilizar plataformas seguras para las transacciones económicas; disponer de una tarjeta diferente para pagos electrónicos y seguir las pautas de seguridad y prevención de la Policía.

Los nuevos gadgets, como smartphones o tablets, se han convertido en potentes herramientas para cometer malas inocentadas. Los especialistas de la Unidad de Investigación Tecnológica (UIT) y del Grupo de Redes Sociales de la Policía Nacional han registrado miles de denuncias, consultas y peticiones de ayuda de los internautas a través de los canales telemáticos de la Policía, como @policia o www.policia.es/colabora.php .

Fraudes, estafas y otros delitos

Un clásico: el Phishing, también sobre cuentas en redes sociales y de correo. Es una de las estafas más habituales y su objetivo es conseguir las claves del internauta para luego obtener beneficios fraudulentos con esos datos. También hay intentos de robo de cuentas en redes sociales o correos electrónicos para luego utilizarlos para realizar spam comercial en su nombre o, lo que es peor, para la distribución de malware.

Ofertas de dinero por realizar transacciones entre cuentas. Sin saberlo, el sujeto se convierte en autor de un delito de blanqueo al ser una "mula" virtual para redes criminales que quieren sacar dinero. Este método consiste en recibir pagos en las cuentas personales de las mulas para luego ingresarlas en otras cuentas o reenviarlas por empresas de transferencias monetarias a cambio de una comisión.

Secuestro virtual de personas en el extranjero, principalmente en países de Sudamérica. Los ciberdelincuentes buscan a un conocido que se encuentre fuera de su país, y no pueda acceder a sus cuentas de correo para contactar con sus familiares y hacerles creer a éstos que el viajero está secuestrado, o que ha tenido un accidente o está enfermo, y solicitar el pago de un rescate inmediato para liberarle o una cantidad de dinero para su atención médica.

Venta de falsas aplicaciones de whatsapp para ordenadores o programas espías. El éxito de esta aplicación para smartphones y su demanda ha empujado a los ciberdelincuentes a vender falsas apps para PCs (que no existen) o programas que supuestamente espían las conversaciones de los contactos. Las víctimas pagan por unas aplicaciones o programas que no existen y que no permiten esos servicios que, como en el caso del supuesto Whatsapp spy, sería además un delito.

Engaño para suscribirte a servicios SMS premium y llamadas a teléfonos de alta tarificación. Los ganchos utilizados son varios: desde supuestos paquetes que no se han recogido a supuestas llamadas de personas que no tienen saldo y requieren contactar con ellos a través de esos medios, falsos premios -gadgets o dinero- en concursos en los que, curiosamente, no se ha participado o mensajes ambiguos de supuestas personas recién separadas y que quieren tomar un café, agregarte supuestamente a Whatsapp o a Facebook.

Chollos que no llegan. Cada vez es más habitual realizar compras a través de Internet y más aún en estas fechas navideñas. La oferta de gangas y chollos de todo tipo de productos entre particulares, o webs de reciente creación, principalmente smartphones, tablets u otros dispositivos electrónicos, que a pesar de haber realizado el pago de la cantidad acordada nunca llegan al destinatario.

Ofertas de trabajo falsas en tiempos de crisis. La fuerte demanda de empleo hace que desaprensivos traten de beneficiarse fraudulentamente de ellos. Peticiones de dinero por adelantado "para el temario o cursos previos del puesto a desempeñar", "para cerrar los trámites de contratación", o pedir que se llame a un teléfono de alto coste o redireccionarle en segunda instancia a ese tipo de números, alargándole la llamada para supuestamente recopilar datos son algunos de las trampas para obtener dinero de la víctima.

El virus que suplanta la identidad de la Policía Nacional, la SGAE o la AEPD sigue activo. Se difunde sobre todo a través de las páginas de descargas y en links acortados distribuidos masivamente con técnicas de ingeniería. Este virus es muy dañino y bloquea el ordenador, inventándose una supuesta multa de 100 € por haber detectado pornografía infantil en el disco duro (hecho que recordemos constituye un delito) o archivos que violan la propiedad intelectual o la Ley Orgánica de Protección de Datos. Se pide el pago a través de medios no rastreables y el usuario, una vez ha abonado, ve que el ordenador no recupera el normal funcionamiento y que ha sido víctima de este engaño.

No seas inocente, no creas en ciberleyendas

Internet, las redes sociales y las aplicaciones de comunicación y mensajería instantánea, como el Whastapp, se han convertido también en una herramienta de difusión para de bulos y ciberleyendas que propagan informaciones falsas que generan alarma entre los destinatarios y que rápidamente se viralizan. El Grupo de Redes Sociales de la Policía ha detectado y recibido numerosas notificaciones sobre mensajes que alertan de la existencia de secuestradores de niños que actúan en una determinada localidad; la distribución de calcomanías o caramelos impregnados de LSD; la venta de colonias a domicilio que adormecen para robar en la vivienda; teléfonos-bomba que son abandonados por terroristas en las calles; mensajes que dicen que si introduces el PIN al revés en un cajero en caso de robo inmediatamente se avisa a la Policía; falsos avisos de colocación de bombas en medios de transporte o centros comerciales, o ritos de iniciación de bandas urbanas o juegos de rol que captan a sus víctimas circulando con las luces apagadas por la carretera. La Policía Nacional recomienda no continuar con la cadena de envíos de este tipo de mensajes y no difundir su contenido a su agenda de contactos. Sólo se debe dar credibilidad a las informaciones difundidas por las Fuerzas y Cuerpos de Seguridad u otras Instituciones oficiales.

Desconfianza racional y sentido común

La Policía Nacional recomienda unas pautas seguras, tanto en el mundo online como offline, para prevenir y evitar ser víctima de estafas, fraudes o timos.

- Actúa con "desconfianza racional" y sentido común ante ofertas o mensajes de fuentes desconocidas. No creas en chollos o gangas y realiza siempre las transacciones económicas a través de plataformas seguras. No compres en webs desconocidas que te lleguen a través de links acortados o fuentes no fiables. Si ves en Internet algún chollo, indaga sobre él. Tanto por la opinión de otros compradores (votos, confianza, trayectoria, etc.) como en cualquier buscador, introduciendo datos por si otros usuarios alertaran de algo raro en dicha oferta

- No des siempre por supuesto que tu interlocutor vía web, correo electrónico o red social es quien dice ser... Ni aunque sea a través de la cuenta reconocida por ti de un amigo tuyo. Puede haber sido "secuestrada" a través de ingeniería social (phishing o malware enmascarado en supuestos archivos muy atractivos)

- Si recibes llamadas perdidas desde un teléfono de alta tarificación (905..., por ejemplo) o de un teléfono normal, pero que te deriva a un 800, toma precauciones. Desconfía también de mensajes inesperados que te lleguen desde un teléfono móvil corto que intenta que interactúes de alguna forma con esa empresa o entidad o que le envíes un SMS con algún texto, sin especificar bien claro las condiciones

- Aquellas supuestas ofertas de trabajo que requieren un desembolso económico previo no son, casi

nunca, reales y esconden un engaño o afán lucrativo a costa de los que buscan empleo. Investiga en Internet el teléfono o características del anuncio

- Si recibes un SMS o un correo pidiendo que actualices tus datos bancarios, de tarjeta o cuenta, no contestes ni rellenes formularios de ningún tipo

- Mantén actualizado tu equipo informático, smartphone o tablet y protegido. Utiliza programas originales y actualiza el sistema operativo, para así evitar la instalación de virus, troyanos, gusanos o programas espía

- Consulta con periodicidad los movimientos de la tarjeta y cuenta bancarias, incluso si dispones de un servicio de alertas tecnológicas al mail o móvil

- Ante la duda, consulta siempre a los agentes de la Policía Nacional en cualquier comisaría de policía o a través de www.policia.es/colabora.php

Datos de contacto:

Nota de prensa publicada en:

Categorías: Nacional