ELEMENTOS COMUNES DE ESTAS ESTAFAS

- La empresa o estafador suele estar en el **extranjero**, no tiene oficinas locales y el usuario nunca ha tenido relación o conocimiento de la empresa.
- El supuesto vendedor se comunica exclusivamente por correo electrónico, y el español utilizado en sus comunicaciones es **deficiente** y parece una traducción automatizada (faltas de ortografía o frases redactadas en lenguaje poco natural).
- Los correos que envían son **plantillas** y apenas están personalizados.
- En algún momento **solicitan un envío de dinero o información personal.**
- En caso de ofertas de trabajo, éstas se ofrecen a distancia (teletrabajo) por **supuestas grandes empresas** que quieren asentarse en el país o que buscan socios inversores.

QUÉ HACER EN CASO DE FRAUDE O DELITO

Si has sido testigo o víctima de un delito informático, puedes **denunciar los hechos a través de Internet** ante el Grupo de Delitos Telemáticos (GDT) de la Guardia Civil (www.gdt.guardiacivil.es) o ante la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional (www.policia.es).

La denuncia **también puede presentarse personalmente** en las dependencias policiales, Guardia Civil o en el juzgado.

Si el usuario únicamente tiene la intención de informar sobre unos hechos que considera ilícitos, **puede hacerlo de forma anónima.**

También se pueden comunicar los hechos a INTECO a fin de informar de los intentos de fraude y localizar así los lugares desde donde se publican páginas, se emiten mensajes fraudulentos o donde se reciben los datos capturados.

FUENTES: Brigada de Investigación Tecnológica (BIT): http://www.policia.es
Grupo de Delitos Telemáticos (GDT): www.gdt.guardiacivil.es
Instituto Nacional de Tecnologías de la Comunicación (INTECO): http://www.inteco.es/
Oficina de Seguridad del Internauta (OSI): www.osi.es

Consejos

1. **NO ABRAS CORREOS DE USUARIOS DESCONOCIDOS** o de servicios que no hayas solicitado. En ningún caso contestes a estos correos y elimínalos directamente.
2. **NO COMPARTAS CONTRASEÑAS**, datos bancarios o personales.
3. **PRECAUCIÓN AL HACER "CLICK" EN ENLACES Y BANNERS** que se faciliten en un correo, foro, web, sms, etc. o al descargar ficheros adjuntos, aunque sean de contactos conocidos; pueden llevarte a sitios web maliciosos o tratarse de ficheros que llevan escondido algún tipo de malware.
4. Cambia las contraseñas, **COMPRUEBA SI SON SEGURAS** e instala un gestor de contraseñas.
5. **HAZ COPIAS DE SEGURIDAD** y verifica que el software del equipo está actualizado. Comprueba que las opciones y herramientas de seguridad (antivirus, cortafuegos...) están actualizadas y bien configuradas.
6. En tu smartphone o tablet utiliza un **CÓDIGO DE BLOQUEO** del terminal. **ANOTA EL CÓDIGO IMEI**, posibilitará el bloqueo del terminal en caso de pérdida o robo. No olvides que **EXISTE MALWARE DISEÑADO ESPECÍFICAMENTE PARA ESTOS DISPOSITIVOS**, por lo que se deben utilizar herramientas de seguridad específicas.
7. En tus compras online verifica que la tienda tiene una web segura y confiable. Las direcciones que comienzan por **"https://" OFRECEN MAYORES GARANTÍAS DE SEGURIDAD.** Toma precauciones en el momento del pago y lee con atención las condiciones de venta. Revisa la información compartida por la web, las facilidades de contacto directo y las opiniones sobre la web o el servicio y si éstas parecen reales o publicitarias.

asgeco CONFEDERACIÓN Asociación General de Consumidores

CONFEDERACIÓN DE CONSUMIDORES Y USUARIOS cecu

GOBIERNO DE ESPAÑA · MINISTERIO DE SANIDAD, SERVICIOS SOCIALES E IGUALDAD · INC INSTITUTO NACIONAL DEL CONSUMO

El presente proyecto ha sido subvencionado por el Ministerio de Sanidad, Servicios Sociales e Igualdad - Instituto Nacional del Consumo, siendo su contenido responsabilidad exclusiva de ASGECO y CECU

FRAUDES Y DELITOS INFORMÁTICOS

RECLAMA!

GANAMOS todos

www.noclamesreclama.org

Introducción

Internet y las nuevas tecnologías han eliminado las barreras espaciales y temporales en las relaciones entre personas, permitiendo compartir el día a día, intercambiar información y documentos, realizar gestiones y compras desde cualquier lugar.

Estas nuevas redes y relaciones a distancia han traído **nuevas formas de delitos y fraudes.** Para evitar sufrir este tipo de problemas, sin dejar de disfrutar de los beneficios que ofrece la red, **es necesario conocer los posibles delitos.**

Si quieres saber más, te sugerimos que visites nuestra página **www.noclamesreclama.org.** Asimismo, podrás encontrar información muy valiosa en la web de la Brigada de Investigación Tecnológica (BIT) de la Policía Nacional, del Grupo de Delitos Telemáticos (GDT) de la Guardia Civil, del Instituto Nacional de Tecnologías de la Comunicación (INTECO, www.inteco.es) y de la Oficina de Seguridad del Internauta (OSI, www.osi.es).

Tipos de delitos y fraudes

PHISHING

Consiste en el **envío de un correo electrónico a un usuario simulando proceder de una entidad legítima y de confianza -red social, banco, institución pública, policía, etc.**- con el objetivo de obtener información personal (contraseñas, datos bancarios o cualquier otra información de interés).

Normalmente, se insta a entrar en la web de dicha entidad a través de un enlace animando al usuario a que introduzca datos personales, número de cuenta, contraseñas, número de seguridad social, etc.

LOTERÍA Y HERENCIAS

Esta estafa consiste en que la víctima **recibe una llamada, un correo electrónico, fax o carta física** de alguien que se hace pasar por representante de una entidad de loterías, despacho de abogados o empresa, normalmente de otro país.

En dicha comunicación se recibe la **información sobre el premio que supuestamente hemos ganado** en un sorteo o una herencia que hemos recibido. La clave para detectar este delito está en que para recibir el premio o herencia tenemos que hacer frente a unos gastos de transferencias y gestión.

PRÉSTAMOS DE DINERO A PARTICULARES

Este tipo delictivo va dirigido a aquellas personas que necesitan urgentemente dinero para hacer frente a pequeños pagos o fianzas y los bancos no les conceden ningún préstamo o crédito o lo hacen a un interés excesivamente alto.

El fraude se materializará cuando la supuesta entidad que hace el préstamo solicita, bajo algún pretexto, el ingreso de una cantidad económica en concepto de, por ejemplo, el pago de un seguro, gastos de gestión del préstamo, adelanto de los intereses de una de las mensualidades o cualquier otro.

PETICIÓN DE DINERO A TRAVÉS DE WEBS DE CONTACTOS

Los delincuentes captan a sus víctimas **a través de páginas de encuentros** o mediante mensajería instantánea. **Se hacen pasar por personas atractivas**, utilizando fotos falsas, y **establecen una relación de confianza** a distancia con la víctima. Una vez ganada la confianza, el delincuente **solicita dinero** por algún concepto: pagar gastos médicos, viajar para conocer a la víctima, escapar de alguna situación en su país o algo similar.

OFERTAS FALSAS DE TRABAJO

Se crea una falsa oferta de trabajo ofreciendo un puesto en buenas condiciones laborales y de salario. La víctima que responde al correo mostrando interés recibirá nuevamente un correo por parte del ciberdelincuente explicándole en qué consiste el trabajo. **Una vez convencido al usuario de la veracidad de la misma, le solicitará una cantidad de dinero en concepto de gastos administrativos, trámites, gestiones, etc.** En este momento se consuma el fraude.

ESTAFAS EN COMPRA DE VEHÍCULOS, ALQUILER DE VIVIENDA Y VENTA DE PRODUCTOS

Este tipo de estafas se basan en ofertas que aparecen en la red y que son **especialmente buenas en su relación calidad/precio** para la adquisición de algún bien o la contratación de un servicio. El fraude consiste en que **el "vendedor" pide, con alguna excusa, adelantar una cantidad.**

Las características más habituales de estos fraudes, además de las comunes, son:

- El vendedor no se encuentra en España.
- El coste del producto/servicio a comprar/contratar es muy inferior al valor de mercado.
- El anuncio contiene fotos genéricas, copiadas de Internet o poseen diferentes marcas de agua.

RANSOMWARE

El más representativo es el llamado "virus de la policía". Este virus, del que circulan varias versiones, **bloquea el ordenador y muestra un mensaje** que parece provenir del Cuerpo Nacional de Policía y que, con la excusa de haber accedido a páginas que contienen pornografía infantil, violación de los derechos de autor u otro tipo de delitos, **solicita cierta cantidad de dinero, en concepto de multa, para desbloquearlo y/o no ser denunciado.**