La AUI elabora una lista con los fraudes más comunes de la Red

- **El robo de identidad encabeza la lista del los fraudes más usados por los cyber-delincuentes. El SPAM el problema que más preocupa y más gastos ocasiona a los usuarios.**

- **El fraude con tarjetas de crédito fue la forma más común reportada.**

- **La Asociación de Usuarios de Internet elabora una guía de recomendaciones a todos los usuarios y en especial a aquellos que crean haber sido víctimas de fraude.**

Madrid, 21 de junio de 2006. La Asociación de Usuarios de Internet, una vez analizadas las quejas del último año, elabora un listado con los fraudes más frecuentes. La reclamación que encabeza la lista es el "robo de identidad" pero son muchas otras las presentadas por los usuarios: subastas en Internet, compras desde el hogar, premios y sorteos, quejas sobre la calidad de los servicios de Internet, oportunidades de trabajo desde casa, préstamos anticipados y servicios telefónicos entre otras. Además en los últimos meses las quejas por fraude que incluyen "transferencia o giro" como método de pago están creciendo con métodos nuevos de phising que combinan el envió masivo de correos con la falsificación de una página que refuerza el reclamo solicitado buscando un mayor número de usuarios que "piquen el anzuelo".

El correo no solicitado, también llamado correo basura o spam, ocupa el primer lugar entre las preocupaciones de los usuarios siendo el que más costes, molestias y desconfianza les genera. "*El coste estimado que supone el Spam para un empleado de una empresa, contabilizando exclusivamente el tiempo que tarda en mirarlo, supone en estos momentos más de 3.500 Euros por trabajador y año. A esto hay que añadir que el 98% de los fraudes y de los problemas de seguridad tiene su origen en un correo no deseado*" apuntó Pérez Subías, presidente de la Asociación.

El segundo problema en este momento está en la falsificación de páginas web. Hay que destacar la respuesta positiva de las entidades financieras y comercios electrónicos que intentan buscar soluciones para combatirlo y para resolver los casos surgidos de estas prácticas en favor de sus clientes. "*En la Asociación creemos que es necesario crear una cultura y unas prácticas que permitan la identificación mutua tanto del usuario como de la aplicación que utilizamos, el reto es conseguirlo de una forma sencilla y segura*".

Robo de identidad

El robo de identidad se produce cuando alguien utiliza la información particular de otra persona, sin su autorización, con fines fraudulentos o para cometer otros delitos en su nombre. "*Obtener la información confidencial de una persona resulta relativamente sencillo*", afirma Pérez Subías, "*robando registros, documentos, correspondencia, mediante el engaño, revolviendo la basura de casa o incluso en los basureros públicos.. También pueden obtener la información a través del correo electrónico, haciéndose pasar por una entidad conocida (phishing) o por teléfono"*.

La dirección de correo electrónico es el medio más utilizado para registrar la identidad de una persona en Internet y suele servir para acumular información de ella. Es muy fácil conseguir direcciones de correo electrónico sin nuestro consentimiento, en foros y chats (ingeniería social).

Los ladrones pueden utilizar su información personal para llamar al emisor de sus tarjetas de crédito para solicitar un cambio de domicilio, puede abrir cuentas a su nombre y extender cheques sin fondos, en definitiva pueden utilizar la información financiera a su antojo. El fraude con tarjetas de crédito fue la forma más común para el robo de identidad, seguido por el fraude de servicios telefónicos (slaming) u otros servicios de utilidades, fraude bancario y fraude relacionado al empleo.

Recomendaciones

La Asociación de Usuarios de Internet recomienda a aquellos que crean haber sido víctimas de este hurto que sigan los siguientes pasos:

- Alertar del fraude a las asociaciones de consumidores, agencia de protección de datos, Instituto Nacional del Consumo, Usuarios de Telecomunicaciones o Cuerpos de Seguridad del Estado.

- Revisar los cargos de nuestras tarjetas. Recordar que el usuario dispone de tres meses para rechazarlos, si no esta de acuerdo, y que la entidad emisora tiene la obligación de devolvernos el dinero.

- Cerrar aquellas tarjetas que crean que han sido falsificadas o abiertas de manera fraudulenta.

- Evitar la acumulación del correo basura, utilizando programas con filtros para separar el correo deseado del SPAM.

- Intentar no abrir los ficheros adjuntos que puedan venir en correo electrónico si no estamos seguros de su procedencia.

- No responder, ni seguir los enlaces de los mensajes fraudulentos que llegan al correo y acceder siempre a las aplicaciones de Internet (banca electrónica, administración,compras…) tecleando su dirección web en el navegador, de esta forma reducimos el riesgo de que nos lleven a una página falsificada. Ningún banco va a solicitar a sus clientes datos financieros ni personales a través de un correo electrónico.

La AUI recomienda obtener la firma electrónica, que es gratuita, para tramitar quejas, denuncias y reclamaciones de forma segura desde nuestro propio ordenador.

Denuncias ante los cuerpos de Seguridad del Estado

Para poder cursar una denuncia ante los cuerpos de Seguridad del Estado, tanto la Dirección General de la Policía Nacional como la Dirección General de la Guardia Civil, se han establecido sistemas telemáticos para la denuncia de delitos tecnológicos, tales como la falsificación y el fraude, la creación y difusión de virus informáticos, la realización de copias piratas de programas o la violación del secreto de las comunicaciones, entre otros. Existen ya una serie de delitos tipificados:

- "**Prop Intelec**" Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

- “**Hacking**” Delitos relacionados con el descubrimiento y revelación del secretos. El acceso ilegal, conseguir secretos de empresas, abusar de los dispositivos y causar daños en el sistema informático, también son hechos que entrañan delito.

- “**Falsificación y fraudes**” Son causa de denuncia todo aquello que implique un delito contra la confidencialidad, la falsificación de documentos, la estafa informática, etc.

- “**Pedofilia**” Delitos relacionados con el contenido. La difusión de la pornografía infantil, la provocación sexual y la prostitución, así como las amenazas, injurias, calumnias, la apología del racismo y la xenofobia son causa de denuncia.

Dónde podemos acudir

- Agencia de Protección de datos https://www.agpd.es/index.php
- Instituto Nacional del Consumo http://www.consumo-inc.es/home/home.htm
- Usuarios de Telecomunicaciones http://www.usuariosteleco.es/
- Unidad de Investigación de la Delincuencia en Tecnologías de la Información (Policía Nacional) https://www.policia.es/bit/index.htm
- Dirección General de la Guardia Civil http://www.gdt.guardiacivil.es/

La Asociación de Usuarios de Internet

La AUI es una entidad sin ánimo de lucro, constituida en Madrid con ámbito nacional el 5 de julio de 1995 y que intenta promover el desarrollo de Internet, de la Sociedad de la Información y de las Nuevas Tecnologías; Proteger y defender los intereses y los derechos de los Usuarios de Internet y de las Nuevas Tecnologías; Fomentar el buen uso de Internet, de las Nuevas Tecnologías y de sus aplicaciones en el hogar, en las empresas y en las Administraciones públicas; tanto para su uso en el ámbito personal como para su uso en actividades profesionales. Actualmente, la página web de la asociación es visitada por más de 13.000 usuarios.

La AUI mantiene un sitio Web donde los usuarios pueden encontrar toda la información necesaria contra los fraudes por Internet. La AUI trabaja a favor de los usuarios para prevenir las prácticas fraudulentas y mejorar la calidad de los servicios de las Telecomunicaciones.

Más Información:

Beatriz Pérez Nuevo
Gabinete de Comunicación

Teléfono de contacto: 91.302.66.32
gabinetedeprensa @ aui.es
http://www.aui.es