

Asociación de Internautas



¿Por qué es importante salvaguardar nuestra identidad digital?

Uno de los delitos que más se están prodigando en la red en los últimos tiempos en el mundo digital es el robo de identidad o usurpación de identidad, la apropiación de la identidad virtual de una persona por un tercero en sus distintas categorías, cómo hacerse pasar por esa persona, asumir su identidad ante otras personas en público o en privado, en general o para aprovechar ciertos recursos como el acceso a la cuenta corriente bancaria, la obtención de créditos o contratación de servicios y/o productos en nombre de la personalidad robada.

Otro caso de usurpación de identidad, posiblemente no delictivo, pero muy engorroso y perjudicial para la imagen, es el utilizado con el fin de perjudicar a una persona, es decir, difamarlo o manchar su nombre con diversos fines que el usurpador busque. En cualquier caso lo más común en estos últimos tiempos se da cuando un tercero, por medios informáticos o personales, obtiene información personal y la utiliza ilegalmente.

Con el mundo digital se han cambiado las tornas, pues si en el mundo físico cuando alguien robaba la cartera o los documentos de identidad la utilización de estos valores tenían unas consecuencias limitadas, en el mundo digital este hecho que se limita al acto de robar determinadas claves de acceso al correo electrónico, cuentas bancarias o acceso al perfil en las redes sociales, cobra una importancia inusitada en el mundo digital porque la presencia física y virtual van de la mano a la hora de acceder a un sinnúmero de prestaciones de servicios y productos por el mero hecho de que el ladrón no tiene que hacerlo presencialmente.

Uno de los más graves inconvenientes es que la persona a la que se la ha robado su identidad no se entera que esto ha sucedido hasta que no se encuentra con las consecuencias que produce el delito cometido.

Las formas en que podemos ser víctimas del robo de nuestra identidad es mediante los correos falsos que recibimos y las técnicas denominadas de phishing . Esta técnica hace pasar a un atacante por una organización, banco o empresa verdaderas para obtener información que garantice acceso a algún recurso que usted utilice en esa organización, banco o empresa.

De forma personal cualquier persona con malas intenciones podría obtener información que escuchó o vio de usted y que le garantice acceso a algún recurso valioso y más directamente acceso a la clave de acceso a Internet en general y determinados servicios en particular.

Como forma habitual de proceder, los atacantes acceden a alguno de los servicios de los que seamos clientes y utilizan directamente a los recursos de esa compañía con nuestros datos personales y secretos, como puedan ser contraseñas, DNI o cuentas bancarias.

Pero ante grandes males existe una buena dosis de remedios que pueden prevenir este tipo de ataques a la identidad personal en el mundo digital y entre los que caben destacar los que recomiendan los expertos y especialmente los que ofrece la Oficina pública de Seguridad del Internauta:

¿Por qué es importante salvaguardar nuestra identidad digital?

- En materia de redes sociales, hay que comprobar los contactos o validar amigos y seguidores antes de agregarlos a nuestros perfiles.

- Obligado es tener mucho cuidado con las redes WiFi públicas a las que te conectas, para no compartir datos sensibles cuando accedes a Internet y por supuesto no compartir desde esos lugares archivos, fotos o vídeos comprometedores o personales.

-Tratar de que la información que emitas viaje cifrada y utilizar cuando emitas información personal solo páginas cuya URL comience por https.

- Prestar atención a las políticas de privacidad y las condiciones de uso de los servicios transaccionales antes de utilizarlos.

- Y muy importante es utilizar claves robustas en todos y cada uno de los servicios que utilicemos en Internet. Una clave robusta tiene como mínimo 8 dígitos en los que se deben combinar números, símbolos y letras y por supuesto no compartir esas claves con nadie. Con nadie.

Y si después de todo nos enteramos que nuestra identidad ha sido robada y/o usurpada, desde la Asociación de Internautas se recomienda actuar de la siguiente manera:

-Si la suplantación o robo de identidad consiste en la publicación de datos personales en Internet, el primer paso es dirigirse a la misma página donde estos aparecen y exigir su cancelación.

-Todos los sitios web o redes sociales tienen apartados para denunciar este tipo de casos.

- Si se trata de que nuestra identidad ha sido utilizada para realizar delitos, fraudes o comportamientos deshonestos es necesario denunciarlo inmediatamente a las fuerzas de seguridad del Estado ya sean los grupos de delitos informáticos de la Policía Nacional o de la Guardia Civil. Acompañando la denuncia con las correspondientes capturas de pantallas y preferiblemente con acta notarial de estos hechos.

Y por último, y en función de si las consecuencias habidas en el hecho del robo y la suplantación tienen consecuencias de carácter legal y jurídico, ponerse en manos de un abogado experto en la resolución de este nuevo tipo de delitos tecnológicos. En cualquier caso la extensión de este nuevo delito llama a que la ciudadanía digital que ahora se conforma se prevenga en buena medida para salvaguardar su identidad digital tan importante como la identidad física tradicional.

Víctor Domingo, presidente de la Asociación de Internautas en [Escritura Pública](#)

2018 ©Asociación de Internautas