DELITOS INFORMÁTICOS | SOCIEDAD | ÚLTIMA PARTE

**La nueva técnica informática que suplanta  
la cara de sus víctimas**

*Mediante el “morphing”, los criminales pueden viajar libremente por fronteras y aduanas, e incluso liberar teléfonos móviles y entrar en páginas web que contengan información confidencial.*

**Por Julián M. Zappia.  
Diplomatic Week.**

La técnica informática Morphing copia y transforma la foto de las víctimas para suplantar su identidad.

Es decir, los estafadores manipulan las fotografías de pasaportes y documentos de identidad de las víctimas con el fin de falsificar estos documentos y burlar los sistemas biométricos faciales de seguridad establecidos en distintos puntos, como, por ejemplo, en los controles de las fronteras, donde recientemente han detectado esta amenaza Europa.

Gracias a este método de falsificación de identidad, los criminales pueden viajar libremente por fronteras y aduanas, además de liberar smartphones y entrar en páginas web que contengan datos confidenciales de sus víctimas.

El morphing se apoya en la Inteligencial Articial, y técnicamente se lo conoce como el procedimiento de interpolar imágenes para formar un espectro en el que cada una de las dos fotografías de partida están a los extremos.

Para crear ese espectro de imágenes intermedias los criminales utilizan una serie de algoritmos que distorsionan la imagen píxel a píxel, con el objetivo de que se vaya pareciendo a la imagen final, aparentemente original y sin modificaciones.

Para la protección ante esta amenaza, el director de autenticación de la compañía WatchGuard Technologies, Alex Cagnoni, aconseja a las posibles víctimas que proporcionen fotos actualizadas para cualquier documento nuevo, y que las empresas, los gobiernos y los controles fronterizos tomen medidas eficaces para la comprobación de la identidad.

Asimismo, también ve necesario implementar la autenticación de dos factores: la biometría facial y el mensaje de confirmación enviado al teléfono móvil del usuario.

En los últimos tiempos, las plataformas virtuales y la tecnología se han convertido en herramienta principal para muchas empresas y personas naturales, con el fin de impulsar y sacar adelante sus proyectos y emprendimientos; no obstante, hay quienes utilizan sus bondades para cometer delitos; el “morphing” es uno de ellos.

La técnica “morphing” se trata de una copia que transforma la foto de las víctimas para suplantar su identidad. Es decir, los ciberdelincuentes manipulan las fotografías de pasaportes y documentos de identidad de las víctimas, con el fin de falsificarlos y poder pasar por alto los sistemas biométricos faciales de seguridad establecidos en distintos puntos como, por ejemplo, aeropuertos y bancos; adicional, puede desbloquear celulares y pasar por las validaciones de aplicaciones bancarias.

Por ello, resulta tan importante entender cómo blindarnos la seguridad ante esta situación y no ser víctimas o blanco fácil de los delincuentes.

Siempre se debe tratar de colocar la activación de tus redes, correos y accesos bancarios con un código de seguridad, aparte de la biometría o la seguridad facial.

Actualizar las fotos de tus documentos con frecuencia es otra opción preventiva, como también en tus redes sociales no aceptar solicitudes de personas desconocidas.

Teniendo en cuenta estas recomendaciones, seguramente habrá una posibilidad más alta de evitar ser un afectado más por el “morphing”.

Aunque hasta el momento es un delito informático en una cantidad pequeña de países, es cuestión de tiempo para que lo sea a nivel global.

En determinadas redes sociales, el uso de aplicaciones de “corrección” de imágenes, rejuvenecimiento o algún otro tipo de filtro fotográfico que altere de alguna forma una imagen en estado original, por el momento, no es considerada como “morphing”.

Pero siempre es adecuado cuidarse y cuidar la imagen personal y privada en redes sociales y otros ámbitos de la red Internet.