Pautas y pistas para cazar ‘deepfakes’

En estos últimos años, se han hecho más conocidas y alcanzables las herramientas de Inteligencia Artificial, las cuales permiten agilizar muchos procesos de trabajo. Ya sea recopilando un gran volumen de información o mecanizando tareas repetitivas, la IA se presenta como un aliado en muchos ámbitos. No obstante, y frente a sus múltiples beneficios, también ha aumentado la presencia del *deepfake*, la manipulación de imágenes, vídeos o audios falsos que simulan ser reales mediante un sofisticado *software* de Inteligencia Artificial.

Desde discursos manipulados que parecen ser dictados por personalidades o políticos reconocidos a imágenes completamente irreales, un uso malicioso de este *software* basado en Inteligencia Artificial se presenta como una amenaza para perpetrar nuevos tipos de fraudes. En este sentido, es esencial estar informado y ser crítico con aquellos contenidos que consumimos para detectar y diferenciar lo que es real de lo que podría tratarse de un *deepfake.*

Por ello, y conocedores de la dificultad a la hora de detectar un *deepfake*, CaixaBank alerta de las señales y pautas que pueden contribuir a la hora de sospechar sobre el origen de un contenido:

1. **Prestar atención al rostro y cuerpo**, ya que el uso del *deepfake* suele centrarse en la cara y las facciones y, por ello, la mala alineación o desproporción con el cuerpo puede hacernos sospechar.
2. **El número de parpadeos puede delatar a los *deepfakes***, puesto que el parpadeo natural supone todo un reto para los softwares de IA que manipulan las imágenes y una ventaja para el usuario a la hora de reconocer si se trata de un vídeo real o manipulado.
3. **Observar hasta el más mínimo detalle facial y de la piel** puede ser esencial para saber si se trata de *deepfake.* Una piel demasiado lisa o arrugada; unas expresiones poco naturales; o una imagen con bordes borrosos puede ser una señal para detectar un fraude.
4. **Analizar el origen de la fuente y su veracidad** es una tarea que nos llevará algunos minutos, pero que será de gran valor para conocer si el origen del vídeo o contenido proviene o no de una fuente fiable.
5. **La extensión de un vídeo se presenta como otra medida para valorar su fiabilidad.** Los deepfakes suelen encontrarse en vídeos cortos y, por ello, si nos encontramos frente a un vídeo de gran duración es más probable que sea real.

CaixaBank, en el apartado de seguridad de su web, explica esta técnica y recomienda que ante cualquier petición singular o sospechosa de alguien conocido recibida en formato de audio o vídeo, lo más recomendable es contactar directamente con la persona en cuestión mediante un canal oficial y asegurarnos de la legitimidad de la solicitud.