Pautes i pistes per caçar *'deepfakes'*

En aquests darrers anys, s'han fet més conegudes i assolibles les eines d'Intel·ligència Artificial, les quals permeten agilitzar molts processos de treball. Ja sigui recopilant un gran volum d'informació o mecanitzant tasques repetitives, la IA es presenta com un aliat en molts àmbits. No obstant, i davant els seus múltiples beneficis, també ha augmentat la presència del *deepfake*, la manipulació d'imatges, vídeos o àudios falsos que simulen ser reals mitjançant un sofisticat *software* d'Intel·ligència Artificial.

Des de discursos manipulats que semblen ser dictats per personalitats o polítics reconeguts a imatges completament irreals, un ús maliciós d'aquest *software* basat en Intel·ligència Artificial es presenta com una amenaça per perpetrar nous tipus de fraus. En aquest sentit, és essencial estar informat i ser crític amb aquells continguts que consumim per detectar i diferenciar el que és real del que podria tractar-se d'un *deepfake*.

Per això, i coneixedors de la dificultat a l'hora de detectar un *deepfake*, CaixaBank alerta dels senyals i pautes que poden contribuir a l'hora de sospitar sobre l'origen d'un contingut:

1. **Prestar atenció al rostre i cos**, ja que l'ús del *deepfake* sol centrar-se en la cara i les faccions i, per això, la mala alineació o desproporció amb el cos pot fer-nos sospitar.
2. **El nombre de parpellejos pot delatar els *deepfakes***, ja que el parpelleig natural suposa tot un repte per als programaris d'IA que manipulen les imatges i un avantatge per a l'usuari a l'hora de reconèixer si es tracta d'un vídeo real o manipulat.
3. **Observar fins al més mínim detall facial i de la pell** pot ser essencial per saber si es tracta de *deepfake*. Una pell massa llisa o arrugada; unes expressions poc naturals; o una imatge amb vores borroses pot ser un senyal per detectar un frau.
4. **Analitzar l'origen de la font i la seva veracitat** és una tasca que ens portarà alguns minuts, però que serà de gran valor per conèixer si l'origen del vídeo o contingut prové o no d'una font fiable.
5. **L'extensió d'un vídeo es presenta com una altra mesura per valorar la seva fiabilitat**. Els *deepfakes* solen trobar-se en vídeos curts i, per això, si ens trobem davant un vídeo de gran durada és més probable que sigui real.

CaixaBank, en l'apartat de seguretat del seu web, explica aquesta tècnica i recomana que davant de qualsevol petició singular o sospitosa d'algú conegut rebuda en format d'àudio o vídeo, el més recomanable és contactar directament amb la persona en qüestió mitjançant un canal oficial i assegurar-nos de la legitimitat de la sol·licitud.