NOTAS OBSERVATORIO DE LA DIGITALIZACIÓN FINANCIERA

FUNCAS – 26 de enero de 2022 **ODF – Funcas 4 / 2022**

¿Cómo usan los ciberdelincuentes el *deepfake* para cometer fraudes bancarios?

En los últimos años viene observándose un aumento del fraude financiero *online*. Esta tendencia se ha acelerado con la pandemia. Se constata como la tecnología *deepfake*, que nació con un fin distinto al de promover el fraude *online*, empieza a ser utilizada para atacar en diversas formas a las empresas, y en particular, a las entidades financieras.

La tecnología *deepfake* se basa en el uso de un conjunto de datos de imágenes, audio y/o vídeo para generar la semejanza de una persona con otra. Gracias al *deepfake* pueden generarse vídeos en los que se ven a personas reales diciendo y haciendo cosas que no dijeron ni hicieron. De hecho, la popularización de esta tecnología tuvo lugar mediante el lanzamiento de algunas campañas publicitarias en las que personajes mediáticos desaparecidos (ej. Lola Flores) aparecían publicitando productos actuales. La cantidad de vídeos *deepfake* publicados ha ido creciendo en los últimos meses. En muchos casos, siendo difundidos en las redes sociales con un tono humorístico.

Esta misma tecnología está siendo ahora utilizada por algunos ciberdelincuentes para suplantar la identidad de potenciales víctimas. Por ejemplo, se han reportado casos conocidos como "fraudes fantasmas", en los que los delincuentes usan datos personales de una persona fallecida para su

beneficio.[1] En otros casos, los ciberdelincuentes usan dicha tecnología para crear identidades falsas o robadas específicamente con el objetivo de abrir cuentas bancarias. En este caso, el delincuente crea un *deepfake* de un solicitante y abre una cuenta *online* con el fin de lavar dinero o de perpetrar otras actividades delictivas. En otros casos, los ciberdelincuentes han usado la voz clonada de un cliente para engañar a algunos de los empleados bancarios y obtener información financiera sensible o para ordenar transacciones.[2]

Ante esta nueva amenaza, muchas entidades financieras están apostando por suscribir acuerdos con empresas FinTech especializadas en esta materia a fin de prevenir estos fraudes.[3] Chase, ABN Amro, Caixabank, Rabobank, ING o Aegon son algunos de los bancos que ya usan tecnologías preventivas para asegurarse de que están tratando con personas reales y no con grabaciones manipuladas.

Combatir estos fraudes es clave para el sector bancario en su conjunto, ya que un crecimiento significativo en el volumen de estos delitos podría lastrar la confianza de los clientes bancarios en la banca digital, en particular cuando gran parte de la contratación y la negociación se desarrolla ya por canales de vídeo o audio.

[1] Haunted by shame: victims of bank transfer scams tell of lasting trauma. The Guardian. 17 abril 2021. https://www.theguardian.com/money/2021/apr/17/bank-transfer-scams-fraud-victims

[2] Fraudsters Cloned Company Director's Voice In $35 Million Bank Heist, Police Find. Forbes. 14 abril 2021. https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/?sh=1d479ece7559

[3] Banks work with fintechs to counter 'deepfake' fraud. Financial Times. 6 septiembre 2020. https://www.ft.com/content/8a5fa5b2-6aac-41cf-aa52-5d0b90c41840